Journal of Combinatorial Theory, Series A 118 (2011) 2185–2206

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Divisible designs and semi-regular relative difference sets from additive Hadamard cocycles

Yu Qing Chen

Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435-0001, United States

ARTICLE INFO

Article history:
Received 23 October 2009
Available online 25 May 2011

Keywords:
Divisible design
Generalized Hadamard matrix
Bent function
Presemifield
Hadamard cocycle
Relative difference set

ABSTRACT

Additive Hadamard cocycles are a natural generalization of presemifields. In this paper, we study divisible designs and semi-regular relative difference sets obtained from additive Hadamard cocycles. We show that the designs obtained from additive Hadamard cocycles are flag transitive. We introduce a new product construction of Hadamard cocycles. We also study additive Hadamard cocycles whose divisible designs admit a polarity in which all points are absolute. Our main results include generalizations of a theorem of Albert and a theorem of Hiramine from presemifields to additive Hadamard cocycles. At the end, we generalize Maiorana–McFarland's construction of bent functions to additive Hadamard cocycles.

1. Introduction

Finite presemifields (or semifields) are important objects in the study of finite geometry as they coordinatize finite translation planes whose dual planes are also translation planes. In [1], Albert introduced the notion of isotopism between non-associative algebras and later proved a fundamental theorem [2, Theorem 6] that presemifields coordinatize isomorphic projective planes if and only if they are isotopic. Hiramine [17] studied p-groups of presemifield type, which are p-groups associated with presemifield planes, and proved an equally important theorem [17, Corollary 5.2] that two p-groups associated with two presemifield planes are isomorphic if and only if the two planes are isomorphic or one plane is isomorphic to the dual plane of the other.

Additive Hadamard cocycles are a natural generalization of presemifields. In this paper, we study symmetric divisible designs and semi-regular relative difference sets obtained from additive Hadamard cocycles. We show that these difference sets are flag transitive and give generalizations of

E-mail address: yuqing.chen@wright.edu.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2011.04.016

[2, Theorem 6] and [17, Corollary 5.2] from presemifields to additive Hadamard cocycles. We will also determine when the designs obtained from additive Hadamard cocycles admit polarities and absolute polarities. In the end, we show some constructions of semi-regular relative difference sets studied in [7] using the intertwining product of additive cocycles introduced in this paper. The main results of this paper are the following two theorems contained in Sections 5 and 6 respectively for all elementary abelian groups H and N.

Theorem 5.5. *Given two additive Hadamard cocycles ψ_1 and ψ_2 of H with coefficients in N, the divisible designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ are isomorphic if and only if the cocycles ψ_1 and ψ_2 are isotopic.*

Theorem 6.2. *Given two additive Hadamard cocycles ψ_1 and ψ_2 of H with coefficients in N such that $|N| > \sqrt{|H|}$, their flag groups $\mathrm{Flag}(\psi_1)$ and $\mathrm{Flag}(\psi_2)$ are isomorphic if and only if the designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ are isomorphic or the designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}^*_{\psi_2}$ are isomorphic.*

The flag group $\mathrm{Flag}(\psi)$ of an additive Hadamard cocycle ψ mentioned in Theorem 6.2 is defined in Section 5 following Corollary 5.2 and discussed in detail in Section 6.

The remainder of the paper is organized as follows. In Section 2, we provide background materials on symmetric divisible designs and relative difference sets, most of which can be found in [4]. In Section 3 we give a general but brief introduction of cocycles of a finite group H with coefficients in a right H-module. We then give a simple proof that the notion of a Hadamard cocycle is equivalent to that of a semi-regular relative difference set with a normal abelian forbidden subgroup. This is the only section of this paper in which cocycles are discussed in their full generality. The remaining sections deal with only cocycles of H whose coefficients are from H-modules having trivial H-actions. The main themes of Section 4 are special properties and product constructions of Hadamard cocycles with coefficients from trivial H-modules, including twisted Kronecker tensor product and twisted intertwining product (Theorem 4.9). In Section 5, we focus on additive Hadamard cocycles and prove Theorem 5.5. In Section 6 we study what we call the flag groups of additive Hadamard cocycles and prove Theorem 6.2. Section 7 contains necessary and sufficient conditions for a symmetric divisible design from an additive Hadamard cocycle to admit polarities and absolute polarities (Theorem 7.1 and Corollaries 7.2 and 7.3). In Section 8, the last section, we introduce the Maiorana–McFarland functions of an additive cocycle and show that they are bent functions if and only if the cocycle is a Hadamard cocycle (Theorem 8.3). We then demonstrate that every odd order flag group of a symmetric divisible design from an additive Hadamard cocycle contains a semi-regular relative difference set R satisfying $1 \in R$ and $rRr = R$ for all $r \in R$. According to [7], such a difference set is unique up to equivalence in a flag group of odd order. In contrast, we exhibit Maiorana–McFarland's bent functions and Dillon's partial spread bent functions as examples (Examples 8.5 and 8.6) for inequivalent semi-regular relative difference sets in elementary abelian 2-groups. These two examples were constructed by Nyberg [26].

2. Symmetric divisible designs and relative difference sets

Combinatorial designs are incidence structures defined on finite sets. Simple examples of such structures are finite projective spaces and affine spaces. Relative difference sets are a special type of *symmetric divisible design* that can be defined as follows.

Definition 2.1. Let m, n, k and λ be positive integers. An (m,n,k,λ)-*divisible design* $\mathfrak{D}$ consists of a finite set $P(\mathfrak{D})$, called point set, together with a family of subsets $B(\mathfrak{D})$, called blocks, of $P(\mathfrak{D})$ such that

(1) $|P(\mathfrak{D})| = mn$ and $P(\mathfrak{D})$ is partitioned into m point classes of size n each.
$|B(\mathfrak{D})| = mn$ and $B(\mathfrak{D})$ is partitioned into m parallel classes of size n each.
(2) Each point in $P(\mathfrak{D})$ is contained in exactly k blocks in $B(\mathfrak{D})$.
Each block in $B(\mathfrak{D})$ contains exactly k points in $P(\mathfrak{D})$.
(3) Given two points p_1 and p_2 in $P(\mathfrak{D})$ of two different point classes, there are exactly λ blocks in $B(\mathfrak{D})$ containing both p_1 and p_2.

Given two blocks b_1 and b_2 in $B(\mathfrak{D})$ of two different parallel classes, there are exactly λ points in $P(\mathfrak{D})$ contained in both b_1 and b_2.

(4) Points from same point class in $P(\mathfrak{D})$ are not joined by any blocks in $B(\mathfrak{D})$.
Blocks from same parallel class in $B(\mathfrak{D})$ have no common points in $P(\mathfrak{D})$.

A *flag* of the design $\mathfrak{D}$ is an *incident pair of a point and a block*, i.e. a pair $\{p, b\}$, $p \in P(\mathfrak{D})$ and $b \in B(\mathfrak{D})$ and $p \in b$. The set of all flags of the design $\mathfrak{D}$ is denoted by $F(\mathfrak{D})$.

One can also use the following more symmetrical but equivalent alternative.

Definition 2.2. Let m, n, k and λ be positive integers. An (m, n, k, λ)-*divisible design* $\mathfrak{D}$ consists of two disjoint finite sets $P(\mathfrak{D})$, called the point set of $\mathfrak{D}$, and $B(\mathfrak{D})$, called the block set of $\mathfrak{D}$, and together with another finite set $F(\mathfrak{D})$, called the flag set of $\mathfrak{D}$, where flags in $F(\mathfrak{D})$ are pairs, called incident pairs, of the form $\{p, b\}$ with $p \in P(\mathfrak{D})$ and $b \in B(\mathfrak{D})$. They satisfy

(1) $|P(\mathfrak{D})| = mn$ and $P(\mathfrak{D})$ is partitioned into m point classes of size n each.
$|B(\mathfrak{D})| = mn$ and $B(\mathfrak{D})$ is partitioned into m parallel classes of size n each.
(2) Each point in $P(\mathfrak{D})$ is incident with exactly k blocks in $B(\mathfrak{D})$.
Each block in $B(\mathfrak{D})$ is incident with exactly k points in $P(\mathfrak{D})$.
(3) Two points in $P(\mathfrak{D})$ of two different point classes are simultaneously incident with exactly λ blocks in $B(\mathfrak{D})$.
Two blocks in $B(\mathfrak{D})$ of two different parallel classes are simultaneously incident with exactly λ points in $P(\mathfrak{D})$.
(4) Two distinct points of same point class in $P(\mathfrak{D})$ are not simultaneously incident with any blocks in $B(\mathfrak{D})$.
Two distinct blocks of same parallel class in $B(\mathfrak{D})$ are not simultaneously incident with any points in $P(\mathfrak{D})$.

From Definition 2.2, it is clear that the *dual design* $\mathfrak{D}^*$ obtained from $\mathfrak{D}$ by exchange the roles of points and blocks, i.e. $P(\mathfrak{D}^*) = B(\mathfrak{D})$, $B(\mathfrak{D}^*) = P(\mathfrak{D})$ and $F(\mathfrak{D}^*) = F(\mathfrak{D})$, is also an (m, n, k, λ)-design. An *isomorphism* $\gamma : \mathfrak{D}_1 \to \mathfrak{D}_2$ between two (m, n, k, λ)-designs $\mathfrak{D}_1$ and $\mathfrak{D}_2$ is a triple $\gamma = (\gamma_p, \gamma_b, \gamma_f)$, where γ_p is a bijection between $P(\mathfrak{D}_1)$ and $P(\mathfrak{D}_2)$ which maps blocks in $B(\mathfrak{D}_1)$ to blocks in $B(\mathfrak{D}_2)$ and $\gamma_b : B(\mathfrak{D}_1) \to B(\mathfrak{D}_2)$ and $\gamma_f : F(\mathfrak{D}_1) \to F(\mathfrak{D}_2)$ are bijections induced from γ_p. Its inverse $\gamma^{-1} : \mathfrak{D}_2 \to \mathfrak{D}_1$ is given by $\gamma^{-1} = (\gamma_p^{-1}, \gamma_b^{-1}, \gamma_f^{-1})$. Two designs $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are said to be *isomorphic* and denoted by $\mathfrak{D}_1 \cong \mathfrak{D}_2$ if there is an isomorphism between the two. Clearly γ induces an isomorphism $\gamma^* : \mathfrak{D}_1^* \to \mathfrak{D}_2^*$, called *dual isomorphism* between the two dual designs, with $\gamma^* = (\gamma_p^*, \gamma_b^*, \gamma_f^*) = (\gamma_b, \gamma_p, \gamma_f)$. An (m, n, k, λ)-design $\mathfrak{D}$ is said to be *self-dual* if $\mathfrak{D} \cong \mathfrak{D}^*$. Given a self-dual (m, n, k, λ)-design $\mathfrak{D}$, an isomorphism $\iota : \mathfrak{D} \to \mathfrak{D}^*$ is called a *polarity* if $\iota_f = \iota_f^{-1}$. A polarity $\iota : \mathfrak{D} \to \mathfrak{D}^*$ is called an *absolute polarity* if every point of $\mathfrak{D}$ is an absolute point, i.e. $\{p, \iota(p)\} \in F(\mathfrak{D})$ for every $p \in P(\mathfrak{D})$. This is equivalent to saying that ι_f fixes mn flags, which is the largest number of flags ι_f can possibly fix.

Given an (m, n, k, λ)-divisible design $\mathfrak{D}$, an isomorphism from $\mathfrak{D}$ to itself is called an *automorphism* of $\mathfrak{D}$. The set of all automorphisms of $\mathfrak{D}$ forms the *automorphism group* $\mathrm{Aut}(\mathfrak{D})$ of $\mathfrak{D}$. Every automorphism of $\mathfrak{D}$ induces an automorphism of $\mathfrak{D}^*$ and vice versa. Hence $\mathrm{Aut}(\mathfrak{D}^*) = \mathrm{Aut}(\mathfrak{D})$ as they are the same set of permutations on the flags of the designs. A subgroup G of $\mathrm{Aut}(\mathfrak{D})$ is called a *Singer group* of $\mathfrak{D}$ if G acts on both $P(\mathfrak{D})$ and $B(\mathfrak{D})$ regularly. When the design $\mathfrak{D}$ admits a Singer group G, we can identify points in $P(\mathfrak{D})$ with elements in G and blocks in $B(\mathfrak{D})$ with subsets of G, and all subsets of G corresponding to blocks in $B(\mathfrak{D})$ are translations of one another by elements of G. The subsets in G corresponding to blocks in $B(\mathfrak{D})$ are called *relative difference sets*. Given a relative difference set R in G, or equivalently, given a block corresponding to R in $B(\mathfrak{D})$, let M_R be the stabilizer in G of the parallel class containing the block R. Then for any other block Rg, a translation of R by $1 \neq g \in G$,

$$|R \cap Rg| = \lambda \quad \text{when } g \notin M_R \quad \text{and} \quad |R \cap Rg| = 0 \quad \text{when } g \in M_R. \tag{1}$$

Since G is also a Singer group of $\mathfrak{D}^*$, if we identify $R \in P(\mathfrak{D}^*) = B(\mathfrak{D})$ with 1 in G, then the points in $P(\mathfrak{D}) = B(\mathfrak{D}^*)$ can be identified with subsets of G. Particularly, since $\{Rr^{-1} \mid r \in R\}$ is the set of all blocks in $B(\mathfrak{D})$ that contains $1 \in G = P(\mathfrak{D})$, the block in $B(\mathfrak{D}^*) = P(\mathfrak{D})$ given by $1 \in G = P(\mathfrak{D})$ is $R^* = \{r^{-1} \mid r \in R\}$. We call R^* the *dual of* R. The block $g \in G = P(\mathfrak{D}) = B(\mathfrak{D}^*)$ of $\mathfrak{D}^*$ is given by R^*g. If N_R is the stabilizer of the point class that contains $1 \in G = P(\mathfrak{D}) = B(\mathfrak{D}^*)$, then for every $1 \neq g \in G$,

$$\left|R^* \cap R^*g\right| = \lambda \quad \text{when } g \notin N_R \quad \text{and} \quad \left|R^* \cap R^*g\right| = 0 \quad \text{when } g \in N_R. \tag{2}$$

Conversely, if a group G of order mn contains a subset R of size k and two subgroups M_R and N_R of order n such that they satisfy both conditions (1) and (2), then one obtains a symmetric (m,n,k,λ)-divisible design $\mathfrak{D}$ with G as its Singer group by letting $P(\mathfrak{D}) = G$ and $B(\mathfrak{D}) = \{Rg \mid g \in G\}$. Such a design is said to be *developed* from R and is denoted by $\mathfrak{D}_R$. Clearly $\mathfrak{D}_R^* \cong \mathfrak{D}_{R^*}$. A difference set R is said to be *fixed by inversion* if $R = R^*$ and such relative difference sets were studied in [3,7,8,20,23]. When R is fixed by inversion, the design $\mathfrak{D}_R$ admits a polarity $\iota : \mathfrak{D}_R \to \mathfrak{D}_R^*$ given by $\iota(g) = Rg \in P(\mathfrak{D}_R^*) = B(\mathfrak{D}_R)$ for every $g \in G = P(\mathfrak{D}_R)$. If $1 \in R$, the polarity ι is an absolute polarity. If the relative difference set R is invariant under every inner automorphism of G, i.e. $g^{-1}rg \in R$ for all $g \in G$ and $r \in R$, then the design $\mathfrak{D}_R$ also admits a polarity $\iota : \mathfrak{D}_R \to \mathfrak{D}_R^*$ given by $\iota(g) = Rg^{-1} \in P(\mathfrak{D}_R^*) = B(\mathfrak{D}_R)$ for every $g \in G$. If one of the two subgroups M_R and N_R of G is normal, then $M_R = N_R$ and condition (1) is equivalent to condition (2) (see Jungnickel [19]). In this paper, we will consider only relative difference sets with $M_R = N_R$ a normal abelian subgroup of G.

A simpler definition of relative difference set when $M_R = N_R$ is normal in G can be stated as follows.

Definition 2.3. A k-element subset R of a group G of order mn is called a (m,n,k,λ)-*relative difference set* relative to a normal subgroup N of order n, called the *forbidden subgroup*, of G if

(i) for every element $g \in G \setminus N$, there are exactly λ pairs of elements $r_1, r_2 \in R$ such that $g = r_1^{-1}r_2$;
(ii) for every $g \in N \setminus \{1\}$, there exist no elements $r_1, r_2 \in R$ such that $g = r_1^{-1}r_2$.

When $k = m$, R is called a *semi-regular* relative difference set.

For more detailed study of relative difference sets, the reader is advised to consult [4] or [28].

Let $\mathrm{Aut}(G)$ be the automorphism group of G and N a subgroup of G. The group $\mathrm{Aut}(G;N)$ is defined to be $\{\alpha \in \mathrm{Aut}(G) \mid \alpha(N) = N\}$. An automorphism $\alpha \in \mathrm{Aut}(G;N)$ is called a *multiplier* of a relative difference set R contained in G relative to N if there is an element $g_\alpha \in G$ such that

$$\alpha(R) := \left\{\alpha(r) \,\middle|\, r \in R\right\} = \{rg_\alpha \mid r \in R\} = Rg_\alpha.$$

Multipliers induce automorphisms of the divisible design $\mathfrak{D}_R$. When α is a multiplier, we will denote $\alpha(g)$ by g^α so that its action on the design $\mathfrak{D}_R$ is consistent with the action of G on $\mathfrak{D}_R$, the right action. If α is a multiplier of R with $R^\alpha = Rg_\alpha$, then $(R^*)^\alpha = (R^\alpha)^* = g_\alpha^{-1}R^*$. For any $g \in G$, let σ_g be the inner automorphism of G given by $x^{\sigma_g} = g^{-1}xg$ for all $x \in G$. Then $(R^*)^{\alpha\sigma_{g_\alpha^{-1}}} = R^*g_\alpha^{-1}$ and therefore $\alpha\sigma_{g_\alpha^{-1}}$ is a multiplier of R^*. If R is fixed by inversion, then $g_\alpha R g_\alpha = R$ and σ_{g_α} is also a multiplier of R.

A symmetric divisible design $\mathfrak{D}$ is said to be flag-transitive if the group $\mathrm{Aut}(\mathfrak{D}) = \mathrm{Aut}(\mathfrak{D}^*)$ acts transitively on $F(\mathfrak{D}) = F(\mathfrak{D}^*)$. A relative difference set R is said to be flag transitive if the design $\mathfrak{D}_R$ is flag transitive.

3. Cocycles and Hadamard cocycles

Using cocycles to study central semi-regular relative difference sets was started by Horadam and de Launey [18] and generalized by Perera and Horadam [27]. A further generalization is given by Galati [14]. Let H be a finite group (written multiplicatively) and N a finite right H-module, i.e. an abelian group N with H acting on N as a group of automorphisms of N such that

(i) $x^1 = x$ for all $x \in N$, where 1 is the identity in H, and
(ii) $(x^{h_1})^{h_2} = x^{h_1 h_2}$ for all $x \in N$ and all $h_1, h_2 \in H$.

Every H-module N is obtained from a homomorphism $s : H \to \mathrm{Aut}(N)$ and $x^h = x^{s(h)}$ for all $h \in H$ and $x \in N$.

Let $\psi : H \times H \to N$ be a map. Then the set $H \times N$ equipped with the binary operation

$$(x_1, y_1) \cdot (x_2, y_2) = \left(x_1 x_2, y_1^{x_2} + y_2 + \psi(x_1, x_2)\right)$$

for all $(x_1, y_1), (x_2, y_2) \in H \times N$ forms a group, which we denote by $E(H, N, \psi)$, if and only if the map ψ satisfies

$$\psi(x_1, x_2)^{x_3} + \psi(x_1 x_2, x_3) = \psi(x_2, x_3) + \psi(x_1, x_2 x_3), \quad \text{for all } x_1, x_2, x_3 \in H. \tag{3}$$

Note that if we set $x_2 = x_3 = 1$ in (3) we get $\psi(x_1, 1) = \psi(1, 1)$; if we set $x_1 = x_2 = 1$ in (3), we get $\psi(1, 1)^{x_3} = \psi(1, x_3)$. Therefore

$$\psi(x_1, 1) = \psi(1, 1) = \psi(1, x_3)^{x_3^{-1}}$$

for all $x_1, x_3 \in H$ when ψ satisfies (3) and the identity element of the group $E(H, N, \psi)$ is $(1, -\psi(1, 1))$. A map satisfying (3) is called a *2-cocycle of H with coefficients in N* (see Brown [5]). Since we are not interested in cocycles in any other dimensions, we will simply call these maps *cocycles*. The cocycles form an abelian group under the natural addition of functions from $H \times H$ to N. This group is usually denoted by $Z(H, N)$. If ψ is a cocycle, then the group N can be embedded in $E(H, N, \psi)$ as a normal abelian subgroup by

$$i : N \to E(H, N, \psi),$$
$$i(y) = \left(1, y - \psi(1, 1)\right), \quad \text{for all } y \in N.$$

On the other hand, if an abelian group N can be embedded as a normal subgroup of a given group G via an embedding $i : N \to G$ and $G/i(N) \cong H$, then N becomes a right H-module with the action $y^h = i^{-1}(\tilde{h}^{-1} i(y) \tilde{h})$ for all $y \in N$ and all $h \in H$, where $\tilde{h}$ is any element in G such that its image in $G/i(N) \cong H$ is h. The action of h does not depend on the choice of $\tilde{h}$ since N is abelian. A transversal function T of N in G is a map from H to G so that $\pi \circ T = 1_H$, where $\pi : G \to G/i(N) = H$ is the natural projection and 1_H is the identity map from H to itself. A transversal of N in G is a subset of G such that the subset intersects with each coset of $i(N)$ in exactly one element. Every transversal function determines a transversal and every transversal gives a transversal function, and we will use the two terms interchangeably. Given a transversal $T : H \to G$, one can define a cocycle

$$\psi_T : H \times H \to N,$$
$$\psi_T(g, h) = i^{-1}\left(T(gh)^{-1} T(g) T(h)\right)$$

and the group G is isomorphic to $E(H, N, \psi_T)$ via an isomorphism

$$f : G \to E(H, N, \psi_T),$$
$$f(g) = \left(\pi(g), i^{-1}\left(T\left(\pi(g)\right)^{-1} g\right)\right), \quad \text{for all } g \in G.$$

The isomorphism f maps the normal abelian subgroup $i(N)$ of G to the normal abelian subgroup $\{(1, y) \mid y \in N\}$ of $E(H, N, \psi_T)$, and the transversal $\{T(x) \mid x \in H\}$ of $i(N)$ in G to the transversal $\{(x, 0) \mid x \in H\}$ of $\{(1, y) \mid y \in N\}$ in $E(H, N, \psi_T)$. Conversely, given a cocycle $\psi : H \times H \to N$, we get a transversal $T = \{(x, 0) \mid x \in H\}$ in the group $E(H, N, \psi)$ and $\psi = \psi_T$. The simplest cocycles of H with coefficients in N are given as follows. Let $\phi : H \to N$ be a map. Then the map

$$\partial\phi : H \times H \to N,$$
$$\partial\phi(g, h) = \phi(g)^h + \phi(h) - \phi(gh)$$

is a cocycle. A cocycle of this form is called a *coboundary*. For instance, if T_1 and T_2 are two transversal functions from $H = G/i(N)$ to G and we define a function $\phi : H \to N$, $\phi(x) = i^{-1}(T_2(x)^{-1}T_1(x))$, then the difference between ψ_{T_1} and ψ_{T_2} is a coboundary, that is the cocycle

$$\psi_{T_1} - \psi_{T_2} : H \times H \to N,$$
$$(\psi_{T_1} - \psi_{T_2})(g,h) = \psi_{T_1}(g,h) - \psi_{T_2}(g,h) = \partial\phi(g,h).$$

The set of coboundaries forms a subgroup of $Z(H,N)$, the group of cocycles, and is usually denoted by $B(H,N)$. The quotient group $Z(H,N)/B(H,N)$ is the second cohomology group $H^2(H,N)$ of H with coefficients in N. The structures of the groups obtained from these simple cocycles are also quite simple. In fact, the group $E(H,N,\partial\phi)$ is isomorphic to $H \ltimes N$. More generally, if two cocycles ψ_1 and ψ_2 differ by a coboundary $\partial\phi$ for some $\phi : H \to N$, i.e. $\psi_1 - \psi_2 = \partial\phi$, then $E(H,N,\psi_1)$ and $E(H,N,\psi_2)$ are isomorphic with the isomorphism

$$f : E(H,N,\psi_1) \to E(H,N,\psi_2),$$
$$f(x,y) = \bigl(x, y + \phi(x)\bigr), \quad \text{for all } x \in H \text{ and all } y \in N. \tag{4}$$

The isomorphism in (4) maps the normal abelian subgroup $\{(1,y) \mid y \in N\}$ of $E(H,N,\psi_1)$ to the normal abelian subgroup $\{(1,y) \mid y \in N\}$ of $E(H,N,\psi_2)$, and the transversal $\{(x,0) \mid x \in H\}$ of $\{(1,y) \mid y \in N\}$ in $E(H,N,\psi_1)$ to the transversal $\{(x,\phi(x)) \mid x \in H\}$ of $\{(1,y) \mid y \in N\}$ in $E(H,N,\psi_2)$. Since for every cocycle $\psi : H \times H \to N$, the constant map $\phi : H \to N$ with $\phi(x) = \psi(1,1)$ for all $x \in H$ gives rise to the coboundary $\partial\phi(g,h) = \psi(1,1)^h$ for $g,h \in H$, we may normalize the cocycle $\psi(g,h)$ by replacing it with $\psi(g,h) - \psi(1,1)^h$. In the remainder of this paper, all cocycles $\psi : H \times H \to N$ and transversal functions $T : H \to G$ are normalized, that is $\psi(1,1) = 0$ and $T(1) = 1$. From (3), all cocycles ψ considered here satisfy

$$\psi(1,h) = \psi(h,1) = \psi(1,1) = 0, \quad \text{for all } h \in H. \tag{5}$$

Given a two-variable map $\psi : H \times H \to N$, we define another two-variable map

$$\psi^* : H \times H \to N,$$
$$\psi^*(g,h) = -\psi\bigl(h^{-1}, g^{-1}\bigr)^{gh}, \quad \text{for all } g,h \in H,$$

and call it the *dual of* ψ. It is easy to check that $(\psi^*)^* = \psi$ and ψ^* is a cocycle if and only if ψ is. In fact if T is a transversal of N in G, then $T^* = \{x^{-1} \mid x \in T\}$ is also a transversal of N in G and $\psi_{T^*} = \psi_T^*$. Note that as a transversal function $T^*(x) = T(x^{-1})^{-1}$ for all $x \in H$. If ψ is a cocycle and we define $\phi_\psi : H \to N$ by $\phi_\psi(x) = \psi(x^{-1}, x)$, then

$$\psi - \psi^* = \partial\phi_\psi.$$

Given two right H-modules N_1 and N_2, one can construct a right H-module $N_1 \oplus N_2$ with $(x_1,x_2)^h = (x_1^h, x_2^h)$ for all $x_1 \in N_1$, $x_2 \in N_2$ and $h \in H$. Similarly, if $\psi_1 : H \times H \to N_1$ and $\psi_2 : H \times H \to N_2$ are two cocycles, then $\psi_1 \oplus \psi_2 : H \times H \to N_1 \oplus N_2$ with $(\psi_1 \oplus \psi_2)(x,y) = (\psi_1(x,y), \psi_2(x,y))$ is also a cocycle.

If $\psi : H \times H \to N$ is a cocycle, we can construct a $|H| \times |H|$ matrix M_ψ whose rows and columns are indexed by the group H and whose entries at (g,h) is $\psi(g,h)^{h^{-1}}$ for all $g,h \in H$. When H is a group of order m and N an abelian group of order n such that $n|m$, we say that a matrix $M = [m(g,h)]_{H \times H}$ whose rows and columns are indexed by H and whose entries $m(g,h)$ are in N is a *generalized Hadamard matrix* if for every $g_1 \neq g_2$ in H and $x \in N$, the number of elements h in H such that $m(g_1,h) - m(g_2,h) = x$ is m/n. Using the Fourier inversion formula, it is easy to see that M is a generalized Hadamard matrix if and only if for every non-principal character χ of N, the matrix $\chi(M) = [\chi(m(g,h))]_{H \times H}$ obtained from M by applying χ to each entry of M satisfies $\chi(M)\overline{\chi(M)}^\top = |H|I$, where $\overline{\chi(M)}^\top$ is the transpose and complex conjugate of $\chi(M)$. By repeatedly using the cocycle identity (3), we have the following lemma.

Lemma 3.1. *Given a cocycle ψ of H with coefficients in N. The following statements are equivalent*:

(i) *for each $u \in H \setminus \{1\}$ and each $x \in N$, the number of elements $v \in H$ such that $\psi(u,v)^{v^{-1}} = x$ is m/n;*
(ii) *for each $v \in H \setminus \{1\}$ and each $x \in N$, the number of elements $u \in H$ such that $\psi(u,v) = x$ is m/n.*

Proof. The statement that for each $1 \neq u \in H$ and each $x \in N$, the number of elements $v \in H$ such that $\psi(u,v)^{v^{-1}} = x$ is m/n is equivalent to the statement that for every $u_1 \neq u_2$ in H and each $x \in N$, the number of elements v in H such that

$$\begin{aligned}
\psi(u_1,v)^{v^{-1}} - \psi(u_2,v)^{v^{-1}} &= \bigl(\psi(u_1,v) - \psi(u_2,v)\bigr)^{v^{-1}} \\
&= \bigl(\psi\bigl(u_1u_2^{-1}, u_2v\bigr) - \psi\bigl(u_1u_2^{-1}, u_2\bigr)^{v}\bigr)^{v^{-1}} \\
&= \psi\bigl(u_1u_2^{-1}, u_2v\bigr)^{v^{-1}} - \psi\bigl(u_1u_2^{-1}, u_2\bigr) \\
&= \bigl[\psi\bigl(u_1u_2^{-1}, u_2v\bigr)^{(u_2v)^{-1}}\bigr]^{u_2} - \psi\bigl(u_1u_2^{-1}, u_2\bigr) \\
&= x
\end{aligned}$$

is m/n. Hence the first statement in the lemma is equivalent to the assertion that M_ψ is a generalized Hadamard matrix, or alternatively, for every non-principal character χ of N, one has $\chi(M_\psi)\overline{\chi(M_\psi)}^\top = |H|I$. Since $\chi(M_\psi)\overline{\chi(M_\psi)}^\top = |H|I$ if and only if $\chi(M_\psi)^\top\overline{\chi(M_\psi)} = |H|I$, one finds that (i) is equivalent to stating that $M_\psi^\top$ is a generalized Hadamard matrix, that is for every $v_1 \neq v_2$ in H and each $x \in N$, the number of elements u in H such that

$$\begin{aligned}
\psi(u,v_1)^{v_1^{-1}} - \psi(u,v_2)^{v_2^{-1}} &= \bigl[\psi(u,v_1) - \psi(u,v_2)^{v_2^{-1}v_1}\bigr]^{v_1^{-1}} \\
&= \bigl[\psi(u,v_1) - \bigl(\psi\bigl(v_2, v_2^{-1}v_1\bigr) + \psi(u,v_1) - \psi\bigl(uv_2, v_2^{-1}v_1\bigr)\bigr)\bigr]^{v_1^{-1}} \\
&= \bigl[\psi\bigl(uv_2, v_2^{-1}v_1\bigr) - \psi\bigl(v_2, v_2^{-1}v_1\bigr)\bigr]^{v_1^{-1}} \\
&= x
\end{aligned}$$

is m/n. Hence (i) and (ii) are equivalent. □

A cocycle $\psi : H \times H \to N$ satisfies (i) or (ii) in Lemma 3.1 is called a *Hadamard cocycle*. Lemma 3.1 shows that

Corollary 3.2. *A cocycle ψ is a Hadamard cocycle if and only if its dual ψ^* is a Hadamard cocycle.*

The following theorem of Galati [14] shows that Hadamard cocycles are essentially semi-regular relative difference sets.

Theorem 3.3. *(See Galati [14].) Let G be a finite group of order mn and N a normal abelian subgroup of order n of G such that $n|m$. Let $R : G/N \to G$ be a transversal function. Then the following statements are equivalent,*

(i) *the transversal $R = \{R(x) \mid x \in G/N\}$ is an $(m,n,m,m/n)$-relative difference set in G relative to N,*
(ii) *the cocycle ψ_R of G/N with coefficients in N is a Hadamard cocycle.*

Proof. The transversal R is an $(m,n,m,m/n)$-relative difference set in G relative to N if and only if for every g in $G \setminus N$, there are m/n pairs of $(h_1,h_2) \in (G/N) \times (G/N)$ such that $g = R(h_1)^{-1}R(h_2) = R(h_1^{-1}h_2)\psi_R(h_1, h_1^{-1}h_2)^{-1}$. Since R is a transversal of N in G, there is a unique x in G/N and a unique y in N such that $g = R(x)y$. Hence the existence of m/n pairs of $(h_1,h_2) \in (G/N) \times (G/N)$ with $g = R(h_1)^{-1}R(h_2)$ for each $g \in G$ is equivalent to the fact that for every $v \neq 1$ in G/N and every $y \in N$, there are m/n elements u in G/N such that $y = \psi_R(u,v)$, i.e. ψ_R is a Hadamard cocycle. Therefore (i) and (ii) are equivalent. □

For any Hadamard cocycle $\psi : H \times H \to N$, the transversal

$$R_\psi = \{(x, 0) \mid x \in H\} \tag{6}$$

of the normal subgroup $\{(1, y) \mid y \in N\}$ of $E(H, N, \psi)$ is a relative difference set as $\psi_{R_\psi} = \psi$. The design developed from R_ψ will be denoted by $\mathfrak{D}_\psi$. If N' is a right H-submodule of N, then the composition map $\psi' : H \times H \to N \to N/N'$ is a cocycle of H with coefficients in N/N', and it is a Hadamard cocycle if ψ is. As a consequence, we have

Proposition 3.4. *If $\psi_1 : H \times H \to N_1$ and $\psi_2 : H \times H \to N_2$ are two cocycles such that $\psi_1 \oplus \psi_2 : H \times H \to N_1 \oplus N_2$ is a Hadamard cocycle, then both $\psi_1 : H \times H \to N_1$ and $\psi_2 : H \times H \to N_2$ are Hadamard cocycles.*

The converse of Proposition 3.4 is not true. Finally, we want mention that a function $f : H \to N$ is called a *bent function* if the coboundary ∂f is a Hadamard cocycle. By (4) f is bent if and only if its graph $\{(x, f(x)) \in H \ltimes N \mid x \in H\}$ is a relative difference set in $H \ltimes N$ relative to N. Hence bent functions are nothing but splitting semi-regular relative difference sets. The term bent function was introduced by Rothaus [29] for $|N| = 2$ and these functions were studied in details by Dillon [11,12] in terms of Hadamard difference sets in elementary abelian 2-groups. Examples with $|N| > 2$ can be found in [9,20,26]. A bent function is said to be *planar* if $|H| = |N|$. Planar functions are extensively studied in [15,16,21,22,25]. When N is a trivial H-module, such a function f is also known as a *perfect non-linear* function.

4. Hadamard cocycles over trivial modules

Starting from this section, for any finite group H, all H-modules N will be trivial, i.e. $x^h = x$ for all $h \in H$ and all $x \in N$. For a trivial H-module N, the cocycle equation (3) becomes

$$\psi(x_1, x_2) + \psi(x_1x_2, x_3) = \psi(x_1, x_2x_3) + \psi(x_2, x_3), \quad \text{for all } x_1, x_2, x_3 \in H. \tag{7}$$

If ψ is a cocycle satisfying Eq. (7), then the subgroup $\{(1, y) \mid y \in N\}$ is contained in the center of $E(H, N, \psi)$, and $\psi^*(x, y) = -\psi(y^{-1}, x^{-1})$ for all x and y in H.

Using the proof of Lemma 3.1, we have the following theorem.

Theorem 4.1. *A cocycle $\psi : H \times H \to N$ is a Hadamard cocycle if and only if for every subgroup N' of N with N/N' cyclic, the map $\pi \circ \psi : H \times H \to N/N'$ is a Hadamard cocycle, where $\pi : N \to N/N'$ is the natural projection.*

Proof. The cocycle $\psi : H \times H \to N$ is a Hadamard cocycle clearly implies that for every subgroup N' of N, the map $\pi \circ \psi : H \times H \to N/N'$ is a Hadamard cocycle. Conversely, if for every subgroup N' of N with N/N' cyclic, the map $\pi \circ \psi : H \times H \to N/N'$ is a Hadamard cocycle, then for every non-principal character χ of N the matrix $\chi(M_\psi)$ satisfies $\chi(M_\psi)\overline{\chi(M_\psi)}^\top = |H|I$, and therefore $\psi : H \times H \to N$ is a Hadamard cocycle. □

Theorem 4.1 can be stated in the following group theoretical way in terms of semi-regular relative difference sets with central forbidden subgroups.

Theorem 4.1′. *Given a finite group G and a central subgroup N of G, a transversal R of N in G is a semi-regular relative difference set relative to N if and only if for every subgroup N' of N with N/N' cyclic, the transversal $\overline{R}$ of N/N' in G/N' obtained from projection of R in G into G/N' is a semi-regular relative difference set relative to N/N'.*

Corollary 4.2. *A function $f : H \to N$ is a bent function if and only if for every subgroup N' of N with N/N' cyclic, the function $\pi \circ f : H \to N/N'$ is a bent function, where $\pi : N \to N/N'$ is the natural projection.*

If N is the additive group of a finite field $\mathbb{F}_q$ of q elements, where q is a power of a prime p, then $\psi : H \times H \to \mathbb{F}_q$ is a Hadamard cocycle if and only if $\mathrm{Tr}(\alpha\psi) : H \times H \to \mathbb{F}_p$ is a Hadamard cocycle for every $\alpha \neq 0$ in $\mathbb{F}_q$, where Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Similarly, a function $f : H \to \mathbb{F}_q$ is a bent function if and only if the function $\mathrm{Tr}(\alpha f) : H \to \mathbb{F}_p$ is a bent function for every $\alpha \neq 0$ in $\mathbb{F}_q$. This is because every cyclic quotient can be obtained from the trace map. Note that if the H-module N is not trivial, Theorem 4.1 may not be true.

Given two groups H and K and an abelian group N, a map $b : H \times K \to N$ from $H \times K$ to N is said to be *bi-multiplicative* (or *bi-additive* if both H and K are abelian and the operations are additions) if

$$b(h_1h_2, k) = b(h_1, k) + b(h_2, k),$$
$$b(h, k_1k_2) = b(h, k_1) + b(h, k_2)$$

for all $h, h_1, h_2 \in H$ and all $k, k_1, k_2 \in K$. The following lemma is easy to verify.

Lemma 4.3. *If $\psi : H \times H \to N$ is bi-multiplicative, then ψ is a cocycle.*

A cocycle in Lemma 4.3 is called a *multiplicative* (or *additive* if H is abelian and its operation is addition) cocycle. In the following special case, the converse of Lemma 4.3 is also true.

Lemma 4.4. *Let $b : H \times K \to N$ be a map. The map*

$$\psi_b (H \times K) \times (H \times K) \to N,$$
$$\psi_b\big((h_1, k_1), (h_2, k_2)\big) = b(h_2, k_1)$$

is a cocycle if and only if b is bi-multiplicative.

Proof. If ψ_b is a cocycle, then $b(1, k) = \psi_b((1, k), (1, 1)) = 0$, $b(h, 1) = \psi_b((1, 1), (h, 1)) = 0$ for all $h \in H$ and $k \in K$, and for every $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$,

$$b(h_2, k_1) + b(h_3, k_1k_2) = b(h_2h_3, k_1) + b(h_3, k_2).$$

When $h_2 = 1$ and $h_3 = h$, one has $b(h, k_1k_2) = b(h, k_1) + b(h, k_2)$. When $k_1 = k$ and $k_2 = 1$, one has $b(h_2h_3, k) = b(h_2, k) + b(h_3, k)$. Hence b is bi-multiplicative. Conversely, if b is bi-multiplicative, then ψ_b is also bi-multiplicative and hence is a cocycle by Lemma 4.3. $\square$

Lemma 4.5. *A multiplicative cocycle ψ of H with coefficients in N is a Hadamard cocycle if and only if for every $h \in H \setminus \{1\}$, the map $\psi(h,\ ) : H \to N$ is onto, if and only if for every $g \in H \setminus \{1\}$, $\psi(\ , g) : H \to N$ is onto.*

Therefore it is relatively easy to obtain Hadamard cocycles from multiplicative ones, and hence semi-regular relative difference sets by Theorem 3.3. Examples of such Hadamard cocycles include presemifields, i.e. additive Hadamard cocycles with $H = N$. However, there are only very restricted families of groups of H and N that provide multiplicative Hadamard cocycles.

Lemma 4.6. *If $\psi : H \times H \to N$ is a multiplicative Hadamard cocycle, then H and N are elementary abelian p-groups for some prime p.*

Proof. We only need to show that H is an elementary abelian p-group as N is a homomorphic image of H. Note that if $f : N \to N'$ is a surjective homomorphism from N to another abelian group N', then $f \circ \psi$ is a multiplicative Hadamard cocycle with coefficients in N' whenever ψ is a multiplicative Hadamard cocycle. Hence, we may assume that $N \cong \mathbb{Z}_p$ for some prime p. Now if H is not elementary abelian, than there is an element $x = y^p \neq 1$ in H for some $y \in H$ or an element $x = y^{-1}z^{-1}xz \neq 1$ in H for some y and z in H. Clearly x lies in the kernel of all homomorphisms $\psi(\ , h) : H \to N$ as $N \cong \mathbb{Z}_p$, i.e. $\psi(x,\ ) : H \to N$ is a 0 map, and this contradicts the fact that ψ is a Hadamard cocycle. $\square$

For cocycles described in Lemma 4.6, we often use addition instead of multiplication for the group operation of H and these cocycles are called *additive Hadamard cocycles*. An additive Hadamard cocycle $\psi : H \times H \to N$ is called a *presemifield* if $H = N$. Such a cocycle is equivalent to a finite translation plane whose dual is also a translation plane.

In [6], we introduced twisted Kronecker tensor product of cocycles. Given cocycles $\psi : H \times H \to N$ and $\phi : K \times K \to N$ and a bi-multiplicative map $b : H \times K \to N$, the twisted Kronecker tensor product of ψ and ϕ twisted by b is the cocycle

$$\psi \otimes_b \phi : (H \times K) \times (H \times K) \to N,$$
$$\psi \otimes_b \phi\big((h_1, k_1), (h_2, k_2)\big) = \psi(h_1, h_2) + b(h_2, k_1) + \phi(k_1, k_2).$$

When $b = 0$, the product $\psi \otimes_0 \phi$ is simply called the Kronecker tensor of ψ and ϕ and denoted by $\psi \otimes \phi$. The following two theorems were proved in [6]. Theorem 4.7 is the constructive version of Theorem 4.8 using cocycles, while Theorem 4.8 is a group theoretical interpretation of Theorem 4.7.

Theorem 4.7. *(See [6, Theorem 3.2].) Let H and K be finite groups and N a finite abelian group. Let $b : H \times K \to N$ be a bi-multiplicative map from $H \times K$ to N and $\psi : H \times H \to N$ and $\phi : K \times K \to N$ be cocycles of H and K respectively with coefficients in N. The twisted Kronecker product $\psi \otimes_b \phi$ of ψ and ϕ twisted by b is a Hadamard cocycle if and only if both ψ and ϕ are Hadamard cocycles.*

Theorem 4.8. *(See [6, Theorem 1.2].) Let G be a finite group and G_1 and G_2 be two normal subgroups of G such that $N = G_1 \cap G_2$ is a central subgroup of G and $G = \langle G_1, G_2\rangle$. Given a transversal R_1 of N in G_1 and a transversal R_2 of N in G_2, the transversal R_1R_2 of N in G is a semi-regular relative difference set in G relative to N if and only if R_1 is a semi-regular relative difference sets in G_1 relative to N and R_2 is a semi-regular relative difference sets in G_2 relative to N.*

In the remainder of this section, we will introduce yet another product construction of Hadamard cocycles. Given two multiplicative cocycles $\psi_1 : H \times H \to N$ and $\psi_2 : H \times H \to N$, and another cocycle $\psi : H \times H \to N$, we define *intertwining product* of ψ_1 and ψ_2, denoted by $\psi_1 \boxtimes \psi_2$, and *twisted intertwining product* of ψ_1 and ψ_2 twisted by ψ, denoted by $\psi_1 \boxtimes_\psi \psi_2$, as follows:

$$\psi_1 \boxtimes \psi_2 : (H \times H) \times (H \times H) \to N,$$
$$\psi_1 \boxtimes \psi_2\big((x_1, y_1), (x_2, y_2)\big) = \psi_1(x_1, y_2) + \psi_2(y_1, x_2),$$

and

$$\psi_1 \boxtimes_\psi \psi_2 : (H \times H) \times (H \times H) \to N,$$
$$\psi_1 \boxtimes_\psi \psi_2\big((x_1, y_1), (x_2, y_2)\big) = \psi_1(x_1, y_2) + \psi(y_1, y_2) + \psi_2(y_1, x_2).$$

Clearly, $\psi_1 \boxtimes_0 \psi_2 = \psi_1 \boxtimes \psi_2$ and $(\psi_1 \boxtimes_\psi \psi_2)^* = \psi_2^* \boxtimes_{\psi^*} \psi_1^*$. Note that instead of using two multiplicative cocycles, if we let ψ_1 and ψ_2 be arbitrary cocycles, the twisted intertwining product $\psi_1 \boxtimes_\psi \psi_2$ may not be a cocycle. We now prove a theorem similar to Theorem 4.7 for the twisted intertwining product.

Theorem 4.9. *Let $\psi_1 : H \times H \to N$ and $\psi_2 : H \times H \to N$ be two multiplicative cocycles, and $\psi : H \times H \to N$ a cocycle. The twisted intertwining product $\psi_1 \boxtimes_\psi \psi_2$ of ψ_1 and ψ_2 twisted by ψ is a Hadamard cocycle if and only if ψ_1 and ψ_2 are Hadamard cocycles.*

Proof. Suppose $\psi_1 : H \times H \to N$ and $\psi_2 : H \times H \to N$ are two additive Hadamard cocycles and $\psi : H \times H \to N$ is a cocycle. Given $(x_1, y_1) \in H \times H$ with $y_1 \neq 1$, for each $y_2 \in H$, there are $|H|/|N|$ of $x_2 \in H$ such that

$$\psi_1 \boxtimes_\psi \psi_2\big((x_1, y_1), (x_2, y_2)\big) = \psi_1(x_1, y_2) + \psi(y_1, y_2) + \psi_2(y_1, x_2) = x \tag{8}$$

as ψ_2 is a Hadamard cocycle. Hence the number of solutions $(x_2, y_2) \in H \times H$ to Eq. (8) is $|H|^2/|N|$. Given $(x_1, y_1) \in H \times H$ with $y_1 = 1$ and $x_1 \neq 1$, the number of solutions $(x_2, y_2) \in H \times H$ to Eq. (8) is clearly $|H|^2/|N|$ as ψ_1 is a Hadamard cocycle. Therefore $\psi_1 \boxtimes_\psi \psi_2$ is a Hadamard cocycle.

Conversely, if $\psi_1 \boxtimes_\psi \psi_2$ is a Hadamard cocycle, then one can see that ψ_1 is a Hadamard cocycle by letting $y_1 = 1$ and ψ_2 is a Hadamard cocycle by letting $y_2 = 1$. $\square$

Unlike Theorem 4.7, Theorem 4.9 does not have a simple group theoretical interpretation similar to Theorem 4.8. Applications of twisted intertwining product will be seen in the last section.

5. Additive Hadamard cocycles and flag transitive relative difference sets

In this section we will exclusively consider additive Hadamard cocycles and the group H will be written additively since it is an elementary abelian group. Many concepts for presemifields can be extended to additive Hadamard cocycles. For example, we say that two additive cocycles ψ_1 and ψ_2 of H with coefficients in N are *isotopic* if there are two automorphisms σ and σ^* in $\mathrm{Aut}(H)$ and one automorphism μ in $\mathrm{Aut}(N)$ such that $\mu(\psi_1(x, y)) = \psi_2(\sigma(x), \sigma^*(y))$. The triple (σ, σ^*, μ) is called an isotopism from ψ_1 and ψ_2. We will show in this section that the relative difference sets derived from additive Hadamard cocycles are flag transitive and two designs from two additive Hadamard cocycles are isomorphic if and only the two cocycles are isotopic.

We first show that relative difference sets obtained from additive Hadamard cocycles possess a large multiplier group.

Lemma 5.1. *If $\psi : H \times H \to N$ is an additive Hadamard cocycle, then for each element $a \in H$, the map $f_a : E(H, N, \psi) \to E(H, N, \psi)$ given by $f_a(x, y) = (x, y + \psi(x, a))$ for all $x \in H$ and $y \in N$ is an automorphism of $E(H, N, \psi)$ and a multiplier of R_ψ defined in* (6)*.*

Proof. It is easy to check that f_a is an automorphism of $E(H, N, \psi)$ for all $a \in H$. when R_ψ is considered as a transversal function, $R_\psi(x) = (x, 0) \in E(H, N, \psi)$ for each $x \in H$, and $f_a(R_\psi(x + a)) = R_\psi(x)R_\psi(-a)^{-1}$ for each $x \in H$ and $a \in H$. Therefore, as a set $f_a(R_\psi) = R_\psi R_\psi(-a)^{-1}$ and f_a is a multiplier of R_ψ. $\square$

The set $K_\psi = \{f_a \mid a \in H\}$ form a subgroup of $\mathrm{Aut}(E(H, N, \psi))$. It is isomorphic to H. Lemma 5.1 shows that

Corollary 5.2. *The group K_ψ acts on the set $\{R_\psi r^{-1} \mid r \in R_\psi\}$ regularly.*

The set $\{R_\psi r^{-1} \mid r \in R_\psi\}$ is the set of all blocks of $B(\mathfrak{D}_\psi)$ containing the point $(0, 0)$ of $P(\mathfrak{D}_\psi) = E(H, N, \psi)$. Let $\mathrm{Flag}(\psi) = K_\psi \ltimes E(H, N, \psi)$. Since $E(H, N, \psi)$ acts on the point set $P(\mathfrak{D}_\psi)$ regularly and K_ψ, the stabilizer of the point $(0, 0)$ in $\mathrm{Flag}(\psi)$, acts on the set of all blocks containing $(0, 0)$ regularly, one has

Theorem 5.3. *If $\psi : H \times H \to N$ is an additive Hadamard cocycle, then R_ψ is a flag-transitive relative difference set and* $\mathrm{Flag}(\psi)$ *acts on $F(\mathfrak{D}_\psi)$ regularly.*

We call $\mathrm{Flag}(\psi)$ the *flag group* of $\mathfrak{D}_\psi$. Our next objective of this section is to extend Albert's result for presemifields in [2] to additive Hadamard cocycles. Given an additive Hadamard cocycle $\psi : H \times H \to N$, the point set of the design $\mathfrak{D}_\psi$ can be identified with $H \times N$, which is the underlying set of $E(H, N, \psi)$. The blocks of $\mathfrak{D}_\psi$ are given by

$$\begin{aligned} R_\psi(s,t) = \big\{(x,0)(s,t) \bigm| x \in H\big\} &= \big\{\big(x+s, t+\psi(x,s)\big) \bigm| x \in H\big\} \\ &= \big\{\big(x, t+\psi(x-s,s)\big) \bigm| x \in H\big\} \\ &= \big\{\big(x, \psi(x,s) + \big(t-\psi(s,s)\big)\big) \bigm| x \in H\big\} \\ &= \big\{\big(x, \psi(x,s)+t'\big) \bigm| x \in H\big\}, \end{aligned}$$

where $t' = t - \psi(s,s)$. Hence the design $\mathfrak{D}_\psi$ can be specified in the following way:

$$P(\mathfrak{D}_\psi) = H \times N = \{p(x,y) \mid x \in H,\ y \in N\}, \tag{9}$$

$$B(\mathfrak{D}_\psi) = H \times N = \{b(s,t) \mid s \in H, t \in N\}, \tag{10}$$

where $b(s,t) = \{p(x, \psi(x,s) + t) \in P(\mathfrak{D}_\psi) \mid x \in H\}$. The coordinates for blocks in $B(\mathfrak{D}_\psi)$ are their slopes and y-intercepts. The point classes of $P(\mathfrak{D}_\psi)$ are $P(c) = \{p(c,y) \in P(\mathfrak{D}_\psi) \mid y \in N\}$ for all $c \in H$, and parallel classes of $B(\mathfrak{D}_\psi)$ are $B(d) = \{b(d,y) \in B(\mathfrak{D}_\psi) \mid y \in N\}$ for all $d \in H$.

Lemma 5.4. *Let ψ_1 and ψ_2 be two additive cocycles of H with coefficients in N and ψ_2 a Hadamard cocycle. Let σ and σ^* be two permutations of H and μ a homomorphism from N to N. if $\mu(\psi_1(x,y)) = \psi_2(\sigma(x), \sigma^*(y))$ for all $x, y \in H$, then σ and σ^* are isomorphisms.*

Proof. For any $x \in H$, one has

$$\begin{aligned}
&\psi_2(\sigma(x), \sigma^*(y_1+y_2) - \sigma^*(y_1) - \sigma^*(y_2)) \\
&\quad = \psi_2(\sigma(x), \sigma^*(y_1+y_2)) - \psi_2(\sigma(x), \sigma^*(y_1)) - \psi_2(\sigma(x), \sigma^*(y_2)) \\
&\quad = \mu(\psi_1(x, y_1+y_2)) - \mu(\psi_1(x,y_1)) - \mu(\psi_1(x,y_2)) \\
&\quad = \mu(\psi_1(x, y_1+y_2) - \psi_1(x,y_1) - \psi_1(x,y_2)) \\
&\quad = 0
\end{aligned}$$

for all $y_1, y_2 \in H$. Since ψ_2 is a Hadamard cocycle and σ is a permutation of H, we get $\sigma^*(y_1+y_2) - \sigma^*(y_1) - \sigma^*(y_2) = 0$ for all $y_1, y_2 \in H$. Therefore σ^* is an isomorphism. Similarly, σ is also an isomorphism. $\square$

We are now ready to prove the following theorem which is a generalization of Albert [2, Theorem 6].

Theorem 5.5. *Given two additive Hadamard cocycles ψ_1 and ψ_2 of H with coefficients in N, the divisible designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ are isomorphic if and only if the cocycles ψ_1 and ψ_2 are isotopic.*

Proof. We use the notation that we set up in (9) and (10) and points and blocks in the design $\mathfrak{D}_{\psi_i}$, $i = 1, 2$, will be denoted by $p_i(x,y)$ and $b_i(s,t)$ respectively.

If ψ_1 and ψ_2 are isotopic, i.e. there are two automorphisms σ and σ^* in $\mathrm{Aut}(H)$ and one automorphism μ in $\mathrm{Aut}(N)$ such that $\mu(\psi_1(x,y)) = \psi_2(\sigma(x), \sigma^*(y))$, define $\gamma_p : P(\mathfrak{D}_{\psi_1}) \to P(\mathfrak{D}_{\psi_2})$, $\gamma_p(p_1(x,y)) = p_2(\sigma(x), \mu(y))$. Then γ_p is a bijection. Also the induced map, which is given by

$$\begin{aligned}
\gamma_b(b_1(s,t)) &= \gamma_b(\{p_1(x, \psi_1(x,s)+t) \mid x \in H\}) \\
&= \{\gamma_p(p_1(x, \psi_1(x,s)+t)) \mid x \in H\} \\
&= \{p_2(\sigma(x), \mu(\psi_1(x,s)) + \mu(t)) \mid x \in H\} \\
&= \{p_2(\sigma(x), \psi_2(\sigma(x), \sigma^*(s)) + \mu(t)) \mid x \in H\} \\
&= \{p_2(x, \psi_2(x, \sigma^*(s)) + \mu(t)) \mid x \in H\} \\
&= b_2(\sigma^*(s), \mu(t))
\end{aligned}$$

for all $b_1(s,t) \in B(\mathfrak{D}_{\psi_1})$, is a bijection between $B(\mathfrak{D}_{\psi_1})$ and $B(\mathfrak{D}_{\psi_2})$. Therefore γ is an isomorphism.

Conversely, if there is an isomorphism γ from $\mathfrak{D}_{\psi_1}$ to $\mathfrak{D}_{\psi_2}$, by composing γ with an element in $\mathrm{Flag}(\psi_2)$, which is transitive on $F(\mathfrak{D}_{\psi_2})$, we can assume that γ_f maps the flag $\{p_1(0,0), b_1(0,0)\}$ in $F(\mathfrak{D}_{\psi_1})$ to the flag $\{p_2(0,0), b_2(0,0)\}$ in $F(\mathfrak{D}_{\psi_2})$. Let $\gamma_p : P(\mathfrak{D}_{\psi_1}) \to P(\mathfrak{D}_{\psi_2})$ be the bijection between the point sets of the two designs with $\gamma_p(p_1(x,y)) = p_2(\sigma(x,y), \mu(x,y))$ for some maps $\sigma : H \times N$

$\to H$ and $\mu : H \times N \to N$. Since γ_p maps a point class $P_1(c) = \{p_1(c, y) \in P(\mathfrak{D}_{\psi_1}) \mid y \in N\}$ of $P(\mathfrak{D}_{\psi_1})$ to a point class $P_2(c') = \{p_2(c', y) \in P(\mathfrak{D}_{\psi_2}) \mid y \in N\}$ of $P(\mathfrak{D}_{\psi_2})$ for some $c' \in H$, this implies that the function σ only depends on the variable $x \in H$ and is independent of $y \in N$, i.e. $\sigma = \sigma(x)$ is an one variable function. Also $\sigma(0) = 0$ as $\gamma_p(p_1(0, 0)) = p_2(0, 0)$. Similarly, since f_b maps parallel blocks in $B(\mathfrak{D}_{\psi_1})$ to parallel blocks in $B(\mathfrak{D}_{\psi_1})$, f_b must map the block $b_1(0, t)$ in $B(\mathfrak{D}_{\psi_1})$, which is parallel to $b_1(0, 0)$, to a block $b_2(0, t')$, which is parallel to $b_2(0, 0)$, in $B(\mathfrak{D}_{\psi_2})$ for some t' in N since $\gamma_b(b_1(0, 0)) = b_2(0, 0)$. Therefore the function μ only depends on the value of $y \in N$, i.e. $\mu = \mu(y)$ and $\mu(0) = 0$. The maps σ and μ are permutations because γ_p is a bijection.

We now show that μ is an isomorphism. Let $s \in H$ and $s \neq 0$. For any $t_1, t_2 \in N$ with $t_1 \neq t_2$, the blocks $b_1(s, t_1)$ and $b_1(s, t_2)$ are two parallel blocks in $B(\mathfrak{D}_{\psi_1})$. Their images

$$\begin{aligned}
\gamma_b\bigl(b_1(s,t_1)\bigr) &= \gamma_b\bigl(\bigl\{p_1\bigl(x, \psi_1(x,s)+t_1\bigr) \in P(\mathfrak{D}_{\psi_1}) \bigm| x \in H\bigr\}\bigr) \\
&= \bigl\{\gamma_p\bigl(p_1\bigl(x, \psi_1(x,s)+t_1\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(\sigma(x), \mu\bigl(\psi_1(x,s)+t_1\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(x, \mu\bigl(\psi_1\bigl(\sigma^{-1}(x),s\bigr)+t_1\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\},
\end{aligned}$$

and

$$\begin{aligned}
\gamma_b\bigl(b_1(s,t_2)\bigr) &= \gamma_b\bigl(\bigl\{p_1\bigl(x, \psi_1(x,s)+t_2\bigr) \in P(\mathfrak{D}_{\psi_1}) \bigm| x \in H\bigr\}\bigr) \\
&= \bigl\{\gamma_p\bigl(p_1\bigl(x, \psi_1(x,s)+t_2\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(\sigma(x), \mu\bigl(\psi_1(x,s)+t_2\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(x, \mu\bigl(\psi_1\bigl(\sigma^{-1}(x),s\bigr)+t_2\bigr)\bigr) \in P(\mathfrak{D}_{\psi_2}) \bigm| x \in H\bigr\},
\end{aligned}$$

must also be parallel blocks. Therefore $\mu(\psi_1(\sigma^{-1}(x), s) + t_1) - \mu(\psi_1(\sigma^{-1}(x), s) + t_2)$ is a constant independent of $x \in H$. Since $\sigma(0) = 0$, we have

$$\mu\bigl(\psi_1\bigl(\sigma^{-1}(x),s\bigr)+t_1\bigr) - \mu\bigl(\psi_1\bigl(\sigma^{-1}(x),s\bigr)+t_2\bigr) = \mu(t_1) - \mu(t_2)$$

for any $s \neq 0$ in H and $t_1, t_2 \in N$. Since $\psi_1(\ ,s) : H \to N$ is a surjective map, one has

$$\mu(t+t_1) - \mu(t+t_2) = \mu(t_1) - \mu(t_2)$$

for all t, t_1 and $t_2 \in N$. If we let $t_2 = 0$, we can see that μ is a homomorphism, and therefore an isomorphism, i.e. $\mu \in \mathrm{Aut}(N)$.

Finally, since $\gamma_p(p_1(0, 0)) = p_2(0, 0)$, all blocks containing $p_1(0, 0)$ in $B(\mathfrak{D}_{\psi_1})$ must be mapped to blocks containing $p_2(0, 0)$ in $B(\mathfrak{D}_{\psi_2})$, that is $\gamma_b(b_1(s, 0)) = b_2(\sigma^*(s), 0)$ for all $s \in H$, where σ^* is a permutation of H with $\sigma^*(0) = 0$. Since

$$\begin{aligned}
\gamma_b\bigl(b_1(s,0)\bigr) &= \gamma_b\bigl(\bigl\{p_1\bigl(x, \psi_1(x,s)\bigr) \bigm| x \in H\bigr\}\bigr) \\
&= \bigl\{\gamma_p\bigl(p_1\bigl(x, \psi_1(x,s)\bigr)\bigr) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(\sigma(x), \mu\bigl(\psi_1(x,s)\bigr)\bigr) \bigm| x \in H\bigr\}
\end{aligned}$$

and

$$\begin{aligned}
b_2\bigl(\sigma^*(s),0\bigr) &= \bigl\{p_2\bigl(x, \psi_2\bigl(x, \sigma^*(s)\bigr)\bigr) \bigm| x \in H\bigr\} \\
&= \bigl\{p_2\bigl(\sigma(x), \psi_2\bigl(\sigma(x), \sigma^*(s)\bigr)\bigr) \bigm| x \in H\bigr\},
\end{aligned}$$

we get $\mu(\psi_1(x, y)) = \psi_2(\sigma(x), \sigma^*(y))$ for all $x, y \in H$. By Lemma 5.4, ψ_1 and ψ_2 are isotopic. $\square$

6. Flag groups

Given an additive Hadamard cocycle $\psi : H \times H \to N$, the flag group $\mathrm{Flag}(\psi) = K_\psi \ltimes E(H, N, \psi)$ can be represented in the following way. As a set, $\mathrm{Flag}(\psi) = H \times H \times N$. The multiplication on $\mathrm{Flag}(\psi)$ is given by

$$\begin{aligned}(s_1, x_1, y_1)(s_2, x_2, y_2) &= \big(s_1 + s_2, x_1 + x_2, y_1 + y_2 + \psi(x_1, s_2) + \psi(x_1, x_2)\big) \\ &= \big(s_1 + s_2, x_1 + x_2, y_1 + y_2 + \psi(x_1, s_2 + x_2)\big).\end{aligned}$$

If we change the coordinates in $H \times H$ by letting $m = s + x$ and $x = x$, then the multiplication on $\mathrm{Flag}(\psi)$ becomes

$$(m_1, x_1, y_1)(m_2, x_2, y_2) = \big(m_1 + m_2, x_1 + x_2, y_1 + y_2 + \psi(x_1, m_2)\big). \tag{11}$$

From the definition of intertwining product given in Section 4, it is clear that the flag group $\mathrm{Flag}(\psi) = E(H \times H, N, 0 \boxtimes \psi)$ and it is the group studied by Hiramine exclusively in [17]. We summarize a few interesting and readily verifiable properties of flag groups in the following proposition. More about flag groups can be found in Theorem 8.4.

Proposition 6.1. *The flag group* $\mathrm{Flag}(\psi) = E(H \times H, N, 0 \boxtimes \psi)$ *has the following properties.*

(i) *The subgroup* $\{(0, 0, b) \mid b \in N\}$ *is the center, the commutator subgroup and, the Frattini subgroup of* $\mathrm{Flag}(\psi)$. *Therefore* $\mathrm{Flag}(\psi)$ *is a special p-group, and, hence, is of nilpotency class* 2.
(ii) *A subgroup of* $\mathrm{Flag}(\psi)$ *is normal if and only if it is contained in* $\{(0, 0, b) \mid b \in N\}$ *or it contains* $\{(0, 0, b) \mid b \in N\}$.
(iii) *The group* $\mathrm{Flag}(\psi)$ *has exponent p if p is odd or exponent* 4 *if* $p = 2$.

Each element (m, x, y) in $\mathrm{Flag}(\psi)$ can be thought of as a flag in $F(\mathfrak{D}_\psi)$ by interpreting m as a slope and (x, y) as a point $p(x, y) \in P(\mathfrak{D}_\psi)$. The point-slope formula determines a unique block $b(m, y - \psi(x, m)) \in B(\mathfrak{D}_\psi)$ and (m, x, y) corresponds to the flag $\{p(x, y), b(m, y - \psi(x, m))\} \in F(\mathfrak{D}_\psi)$. The action of $\mathrm{Flag}(\psi)$ on $P(\mathfrak{D}_\psi)$ is given by

$$\big(p(x, y)\big)(m, u, v) = p\big(x + u, y + v + \psi(x, m)\big)$$

for all $p(x, y) \in P(\mathfrak{D}_\psi)$ and all $(m, u, v) \in \mathrm{Flag}(\psi)$. The induced action of $\mathrm{Flag}(\psi)$ on $B(\mathfrak{D}_\psi)$ is given by

$$\begin{aligned}\big(b(s, t)\big)(m, u, v) &= \big\{\big(p\big(x, t + \psi(x, s)\big)\big)(m, u, v) \bigm| x \in H\big\} \\ &= \big\{p\big(x + u, t + v + \psi(x, s) + \psi(x, m)\big) \bigm| x \in H\big\} \\ &= \big\{p\big(x, t + v + \psi(x - u, s + m)\big) \bigm| x \in H\big\} \\ &= \big\{p\big(x, t + v - \psi(u, s + m) + \psi(x, s + m)\big) \bigm| x \in H\big\} \\ &= b\big(s + m, t + v - \psi(u, s + m)\big)\end{aligned}$$

for all $b(s, t) \in B(\mathfrak{D}_\psi)$ and all $(m, u, v) \in \mathrm{Flag}(\psi)$. The action of $\mathrm{Flag}(\psi)$ on $F(\mathfrak{D}_\psi)$ is consistent with the right multiplication of $\mathrm{Flag}(\psi)$. If we denoted by $p^*(x, y)$ and $b^*(s, t)$ the points and blocks of the design $\mathfrak{D}_{\psi^*}$ as in (9) and (10) with ψ being replaced by ψ^*, then there is a canonical isomorphism $c : \mathfrak{D}_{\psi^*} \to \mathfrak{D}_\psi^*$ with $c_p(p^*(u, v)) = b(u, v) \in P(\mathfrak{D}_\psi^*) = B(\mathfrak{D}_\psi)$ for all $p^*(u, v) \in P(\mathfrak{D}_{\psi^*})$, $c_b(b^*(u, v)) = p(u, v) \in B(\mathfrak{D}_\psi^*) = P(\mathfrak{D}_\psi)$ for all $b^*(u, v) \in B(\mathfrak{D}_{\psi^*})$, and

$$c_f(m, x, y) = \big(x, m, y + \psi(m, x)\big) \in \mathrm{Flag}(\psi) = F(\mathfrak{D}_\psi) = F\big(\mathfrak{D}_\psi^*\big) \tag{12}$$

for all $(m, x, y) \in \mathrm{Flag}(\psi^*) = F(\mathfrak{D}_{\psi^*})$. In fact, the bijection $c_f : \mathrm{Flag}(\psi^*) \to \mathrm{Flag}(\psi)$ is a group isomorphism.

There are two important elementary abelian subgroups in $\mathrm{Flag}(\psi)$, the stabilizer of $p(0,0)$ and that of $b(0,0)$. The stabilizer of $p(0,0)$ is $S_p = \{(m,0,0) \in \mathrm{Flag}(\psi) \mid m \in H\}$ and the stabilizer of $b(0,0)$ is $S_b = \{(0,a,0) \in \mathrm{Flag}(\psi) \mid a \in H\}$. The flag group $\mathrm{Flag}(\psi)$ is generated by S_p and S_b. Let

$$\mathrm{Aut}\big(\mathrm{Flag}(\psi); S_p, S_b\big) = \big\{\alpha \in \mathrm{Aut}\big(\mathrm{Flag}(\psi)\big) \bigm| \alpha(S_p) = S_p \text{ and } \alpha(S_b) = S_b\big\}.$$

It is easy to check that there is an one-to-one correspondence between automorphisms of $\mathrm{Flag}(\psi)$ in $\mathrm{Aut}(\mathrm{Flag}(\psi); S_p, S_b)$ and isotopisms between ψ and itself. From the proof of Theorem 5.5 one has that

$$\mathrm{Aut}(\mathfrak{D}_\psi) = \mathrm{Flag}(\psi) \rtimes \mathrm{Aut}\big(\mathrm{Flag}(\psi); S_p, S_b\big).$$

The following theorem is a generalization of the result of Hiramine [17, Corollary 5.2].

Theorem 6.2. *Given two additive Hadamard cocycles ψ_1 and ψ_2 of H with coefficients in N such that $|N| > \sqrt{|H|}$, their flag groups $\mathrm{Flag}(\psi_1)$ and $\mathrm{Flag}(\psi_2)$ are isomorphic if and only if the designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ are isomorphic or the designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}^*_{\psi_2}$ are isomorphic.*

Proof. Let $f : \mathrm{Flag}(\psi_1) \to \mathrm{Flag}(\psi_2)$ be an isomorphism. Since $\{(0,0,b) \in F(\psi_i) \mid b \in N\}$ is the center of $\mathrm{Flag}(\psi_i)$ for both $i = 1$ and $i = 2$, $f(\{(0,0,b) \in \mathrm{Flag}(\psi_1) \mid b \in N\}) = \{(0,0,b) \in \mathrm{Flag}(\psi_2) \mid b \in N\}$. If we let

$$f(m,a,b) = \big(f_1(m,a,b), f_2(m,a,b), f_3(m,a,b)\big),$$

where $f_1(m,a,b)$ and $f_2(m,a,b)$ are in H and $f_3(m,a,b)$ is in N, then the functions f_1, f_2 and f_3 satisfy $f_1(0,0,b) = f_2(0,0,b) = 0$. Since f is an isomorphism, we have $f((m_1,a_1,b_1)(m_2,a_2,b_2)) = f(m_1,a_1,b_1)f(m_2,a_2,b_2)$, i.e.

$$f\big(m_1+m_2, a_1+a_2, b_1+b_2+\psi_1(a_1,m_2)\big) = f(m_1,a_1,b_1)f(m_2,a_2,b_2),$$

for all (m_1,a_1,b_1) and (m_2,a_2,b_2) in $\mathrm{Flag}(\psi_1)$. This is equivalent to

$$f_1\big(m_1+m_2, a_1+a_2, b_1+b_2+\psi_1(a_1,m_2)\big) = f_1(m_1,a_1,b_1) + f_1(m_2,a_2,b_2), \tag{13}$$

$$f_2\big(m_1+m_2, a_1+a_2, b_1+b_2+\psi_1(a_1,m_2)\big) = f_2(m_1,a_1,b_1) + f_2(m_2,a_2,b_2), \tag{14}$$

$$\begin{aligned} &f_3\big(m_1+m_2, a_1+a_2, b_1+b_2+\psi_1(a_1,m_2)\big) \\ &\quad = f_3(m_1,a_1,b_1) + f_3(m_2,a_2,b_2) + \psi_2\big(f_2(m_1,a_1,b_1), f_1(m_2,a_2,b_2)\big) \end{aligned} \tag{15}$$

for all $m_1, m_2, a_1, a_2 \in H$ and $b_1, b_2 \in N$,

In order to prove the existence of an isotopism between ψ_1 and ψ_2 or ψ_2^*, we will further decompose the maps f_1, f_2 and f_3. If we choose $m_2 = a_2 = 0$ in (13), (14) and (15), we get

$$f_1(m_1,a_1,b_1+b_2) = f_1(m_1,a_1,b_1),$$

$$f_2(m_1,a_1,b_1+b_2) = f_2(m_1,a_1,b_1),$$

$$f_3(m_1,a_1,b_1+b_2) = f_3(m_1,a_1,b_1) + f_3(0,0,b_2),$$

for all $m_1, a_1 \in H$ and all $b_1, b_2 \in N$. Therefore, the maps f_1 and f_2 are independent of b and they are homomorphisms, and $(f_1, f_2) : H \times H \to H \times H$ is an isomorphism. Let $s : H \times H \to N$ be the map $s(m,a) = f_3(m,a,0)$ and $\mu : N \to N$ be the map $\mu(b) = f_3(0,0,b)$. Set $b_1 = 0$ in $f_3(m_1,a_1,b_1+b_2) = f_3(m_1,a_1,b_1) + f_3(0,0,b_2)$, we get $f_3(m,a,b) = s(m,a) + \mu(b)$. Hence $s(m_1,a_1) + \mu(b_1+b_2) = s(m_1,a_1) + \mu(b_1) + \mu(b_2)$ and μ is a homomorphism. In fact μ is an isomorphism because $f(\{(0,0,b) \in \mathrm{Flag}(\psi_1) \mid b \in N\}) = \{(0,0,b) \in \mathrm{Flag}(\psi_2) \mid b \in N\}$. Now the equation $f_3(m_1+m_2, a_1+a_2, b_1+b_2+\psi_1(a_1,m_2)) = f_3(m_1,a_1,b_1) + f_3(m_2,a_2,b_2) + \psi_2(f_2(m_1,a_1,b_1), f_1(m_2,a_2,b_2))$ is equivalent to

$$\begin{aligned} &s(m_1+m_2,a_1+a_2)+\mu\big(\psi_1(a_1,m_2)\big)\\ &\quad =s(m_1,a_1)+s(m_2,a_2)+\psi_2\big(f_2(m_1,a_1),\, f_1(m_2,a_2)\big) \end{aligned}\tag{16}$$

for all (m_1,a_1) and (m_2,a_2) in $H\times H$. If we switch (m_1,a_1) and (m_2,a_2) to get a new equation and cancel all terms involving the function s in the new equation with those in (16), we get

$$\begin{aligned} &\mu\big(\psi_1(a_1,m_2)\big)+\psi_2\big(f_2(m_2,a_2),\, f_1(m_1,a_1)\big)\\ &\quad =\mu\big(\psi_1(a_2,m_1)\big)+\psi_2\big(f_2(m_1,a_1),\, f_1(m_2,a_2)\big) \end{aligned}\tag{17}$$

for all (m_1,a_1), and (m_2,a_2) in $H\times H$. Define four homomorphisms $u_1,u_2,v_1,v_2:H\to H$ given by

$$u_1(x)=f_1(x,0);\qquad u_2(x)=f_2(x,0);\qquad v_1(x)=f_1(0,x);\qquad v_2(x)=f_2(0,x)$$

for all $x\in H$. Then $f_1(m,a)=u_1(m)+v_1(a)$ and $f_2(m,a)=u_2(m)+v_2(a)$ for all $m,a\in H$. Substituting f_1 and f_2 in (17) with these formulas, we get

$$\begin{aligned} &\mu\big(\psi_1(a_1,m_2)\big)+\psi_2\big(u_2(m_2),u_1(m_1)\big)+\psi_2\big(u_2(m_2),\,v_1(a_1)\big)\psi_2\big(v_2(a_2),u_1(m_1)\big)\\ &\qquad +\psi_2\big(v_2(a_2),\,v_1(a_1)\big)\\ &\quad =\mu\big(\psi_1(a_2,m_1)\big)+\psi_2\big(u_2(m_1),u_1(m_2)\big)+\psi_2\big(u_2(m_1),\,v_1(a_2)\big)\psi_2\big(v_2(a_1),u_1(m_2)\big)\\ &\qquad +\psi_2\big(v_2(a_1),\,v_1(a_2)\big). \end{aligned}\tag{18}$$

If we let $a_1=m_2=0$ in (18), we get

$$\psi_2\big(v_2(a_2),u_1(m_1)\big)=\mu\big(\psi_1(a_2,m_1)\big)+\psi_2\big(u_2(m_1),v_1(a_2)\big).\tag{19}$$

If we let $a_2=m_1=0$ in (18), we get

$$\mu\big(\psi_1(a_1,m_2)\big)+\psi_2\big(u_2(m_2),v_1(a_1)\big)=\psi_2\big(v_2(a_1),u_1(m_2)\big).\tag{20}$$

Combining Eqs. (18), (19) and (20), we get

$$\mu\big(\psi_1(x,y)\big)=\psi_2\big(v_2(x),u_1(y)\big)-\psi_2\big(u_2(y),v_1(x)\big),\tag{21}$$

$$\psi_2\big(u_2(x),u_1(y)\big)=\psi_2\big(u_2(y),u_1(x)\big),\tag{22}$$

$$\psi_2\big(v_2(x),v_1(y)\big)=\psi_2\big(v_2(y),v_1(x)\big)\tag{23}$$

for all $x,y\in H$.

We are now going to obtain an isotopism between ψ_1 and ψ_2 or ψ_2^*. Since $(f_1,f_2):H\times H\to H\times H$ is an isomorphism, the intersection of the kernels $\operatorname{Ker}(u_1)\cap\operatorname{Ker}(u_2)=0$. If $\operatorname{Ker}(u_1)\neq 0$ and $0\neq h\in\operatorname{Ker}(u_1)$, then by (22), we get $\psi_2(u_2(h),u_1(y))=\psi_2(u_2(y),u_1(h))=0$ for all $y\in H$, and hence $\operatorname{Im}(u_1)$, the image of u_1, is contained in the kernel of $\psi_2(u_2(h),\ )$. Since ψ_2 is an additive Hadamard cocycle and $u_2(h)\neq 0$ as $u_1(h)=0$, the size of the kernel of $\psi_2(u_2(h),\ )$ is $|H|/|N|$. Therefore $|\operatorname{Im}(u_1)|=|H|/|\operatorname{Ker}(u_1)|\leqslant |H|/|N|$, and consequently $|\operatorname{Ker}(u_1)|\geqslant |N|>\sqrt{|H|}$. Similarly, if $\operatorname{Ker}(u_2)\neq 0$, then by (23), we have $|\operatorname{Ker}(u_2)|>\sqrt{|H|}$. From $\operatorname{Ker}(u_1)\cap\operatorname{Ker}(u_2)=0$, at least one of u_1 and u_2 is an isomorphism. If u_1 is an isomorphism, then by (21), we find that

$$\begin{aligned} \mu\big(\psi_1(x,y)\big)&=\psi_2\big(v_2(x),u_1(y)\big)-\psi_2\big(u_2(y),v_1(x)\big)\\ &=\psi_2\big(v_2(x),u_1(y)\big)-\psi_2\big(u_2(y),u_1\big(u_1^{-1}v_1(x)\big)\big)\\ &=\psi_2\big(v_2(x),u_1(y)\big)-\psi_2\big(u_2\big(u_1^{-1}v_1(x)\big),u_1(y)\big)\\ &=\psi_2\big(v_2(x)-u_2\big(u_1^{-1}v_1(x)\big),u_1(y)\big)\\ &=\psi_2\big(\big(v_2-u_2u_1^{-1}v_1\big)(x),u_1(y)\big) \end{aligned}$$

for all $x, y \in H$. Since both ψ_1 and ψ_2 are additive Hadamard cocycles and μ is an isomorphism, the homomorphism $v_2 - u_2 u_1^{-1} v_1$ must be an isomorphism and ψ_1 and ψ_2 are isotopic, and by Theorem 5.5, $\mathfrak{D}_{\psi_1} \cong \mathfrak{D}_{\psi_2}$. Similarly, if u_2 is an isomorphism, we can show that $\mathfrak{D}_{\psi_1} \cong \mathfrak{D}_{\psi_2^*} = \mathfrak{D}_{\psi_2}^*$.

Conversely, if $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ are isomorphic, then by Theorem 5.5, there is an isotopism (σ, σ^*, μ) such that $\mu(\psi_1(x, y)) = \psi_2(\sigma(x), \sigma^*(y))$ for all $x, y \in H$, and one can easily check that the map $f : \mathrm{Flag}(\psi_1) \to \mathrm{Flag}(\psi_2)$ given by $f(m, a, b) = (\sigma^*(m), \sigma(a), \mu(b))$ for all $(m, a, b) \in \mathrm{Flag}(\psi_1)$ is a group isomorphism. Similarly, if $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}^*$ are isomorphic, then $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2^*}$ are isomorphic and $\mathrm{Flag}(\psi_1) \cong \mathrm{Flag}(\psi_2^*) \cong \mathrm{Flag}(\psi_2)$. $\square$

Remark 6.3. The condition $|N| > \sqrt{|H|}$ does not seem to be very natural but we do not have a proof without this condition. The theorem is true for all Hadamard cocycles $\psi : H \times H \to N$ when N is of prime order p because all such cocycles are isotopic and all flag groups of such cocycles are isomorphic as they are extra special p-groups of exponent p when p is odd, or central products of dihedral groups of order 8 when $p = 2$. We incline to believe that the theorem is probably still true without the condition.

7. Polarities of designs from additive Hadamard cocycles

From the proof of Theorem 5.5, one can see that in general if the designs $\mathfrak{D}_{\psi_1}$ and $\mathfrak{D}_{\psi_2}$ obtained from two additive Hadamard cocycles ψ_1 and ψ_2 are isomorphic, any isomorphism $\gamma : \mathfrak{D}_{\psi_1} \to \mathfrak{D}_{\psi_2}$ is given by elements $a, a^* \in H$, $b \in N$, $\sigma, \sigma^* \in \mathrm{Aut}(H)$, $\mu \in \mathrm{Aut}(N)$ such that $\mu(\psi_1(x, y)) = \psi_2(\sigma(x), \sigma^*(y))$ and the map $\gamma_f : F(\mathfrak{D}_{\psi_1}) \to F(\mathfrak{D}_{\psi_2})$ is given by

$$\gamma_f(m, x, y) = \bigl(\sigma^*(m) + a^*, \sigma(x) + a, \mu(y) + b + \psi_2\bigl(\sigma(x), a^*\bigr)\bigr).$$

Hence $\gamma_f^{-1} : F(\mathfrak{D}_{\psi_2}) \to F(\mathfrak{D}_{\psi_1})$ is given by

$$\begin{aligned}\gamma_f^{-1}(m, x, y) = \bigl(&\sigma^{*-1}(m) + \sigma^{*-1}\bigl(-a^*\bigr), \sigma^{-1}(x) + \sigma^{-1}(-a), \mu^{-1}(y) + \mu^{-1}(-b)\\ &+ \psi_1\bigl(\sigma^{-1}(x), \sigma^{*-1}\bigl(-a^*\bigr)\bigr) + \psi_1\bigl(\sigma^{-1}(a), \sigma^{*-1}\bigl(a^*\bigr)\bigr)\bigr).\end{aligned}$$

If $\mathfrak{D}_\psi$ is self-dual, then $\mathfrak{D}_\psi \cong \mathfrak{D}_\psi^* \cong \mathfrak{D}_{\psi^*}$ and by Theorem 5.5, ψ and ψ^* are isotopic. Since every isomorphism $\iota : \mathfrak{D}_\psi \to \mathfrak{D}_\psi^*$ can be decomposed into $\iota = c \circ \gamma$, where $c : \mathfrak{D}_{\psi^*} \to \mathfrak{D}_\psi^*$ is the canonical isomorphism (see (12)) and $\gamma : \mathfrak{D}_\psi \to \mathfrak{D}_{\psi^*}$ is the isomorphism $c^{-1} \circ \iota$ given by some elements $a, a^* \in H$, $b \in N$, $\sigma, \sigma^* \in \mathrm{Aut}(H)$, $\mu \in \mathrm{Aut}(N)$ such that $\mu(\psi(x, y)) = \psi^*(\sigma(x), \sigma^*(y))$, the permutations ι_f and ι_f^{-1} of $F(\mathfrak{D}_\psi) = F(\mathfrak{D}_\psi^*)$ are given by

$$\begin{aligned}\iota_f(m, x, y) &= c_f\bigl(\gamma_f(m, x, y)\bigr)\\ &= c_f\bigl(\sigma^*(m) + a^*, \sigma(x) + a, \mu(y) + b + \psi^*\bigl(\sigma(x), a^*\bigr)\bigr)\\ &= \bigl(\sigma(x) + a, \sigma^*(m) + a^*, \mu(y) + b + \psi^*\bigl(\sigma(x), a^*\bigr)\\ &\quad + \psi\bigl(\sigma^*(m) + a^*, \sigma(x) + a\bigr)\bigr)\end{aligned}\tag{24}$$

and

$$\begin{aligned}\iota_f^{-1}(m, x, y) &= \gamma_f^{-1}\bigl(c_f^{-1}(m, x, y)\bigr)\\ &= \gamma_f^{-1}\bigl(x, m, y - \psi(x, m)\bigr)\\ &= \bigl(\sigma^{*-1}(x) + \sigma^{*-1}\bigl(-a^*\bigr), \sigma^{-1}(m) + \sigma^{-1}(-a), \mu^{-1}(y) - \mu^{-1}\bigl(\psi(x, m)\bigr)\\ &\quad + \mu^{-1}(-b) + \psi\bigl(\sigma^{-1}(m), \sigma^{*-1}\bigl(-a^*\bigr)\bigr) + \psi\bigl(\sigma^{-1}(a), \sigma^{*-1}\bigl(a^*\bigr)\bigr)\bigr),\end{aligned}\tag{25}$$

for all $(m, x, y) \in F(\mathfrak{D}_\psi) = F(\mathfrak{D}_\psi^*)$.

Theorem 7.1. *Let ψ be an additive Hadamard cocycle. The design $\mathfrak{D}_\psi$ has a polarity if and only if ψ is isotopic to an additive Hadamard cocycle ϕ such that $\mu \circ \phi = \phi^*$, for some $\mu \in \mathrm{Aut}(N)$ satisfying $\mu^2 = 1$.*

Proof. If $\mathfrak{D}_\psi$ is self-dual and $\iota : \mathfrak{D}_\psi \to \mathfrak{D}_\psi^*$ is a polarity given by $a, a^* \in H$, $b \in N$, $\sigma, \sigma^* \in \mathrm{Aut}(H)$, $\mu \in \mathrm{Aut}(N)$, as in (24), such that $\mu(\psi(x, y)) = \psi^*(\sigma(x), \sigma^*(y))$, then $\iota_f = \iota_f^{-1}$. By (24) and (25), one has $\sigma^* = \sigma^{-1}$, $a^* = -\sigma^{-1}(a)$, $\mu^2 = 1$, and $\mu(b) = -b$. Hence $\mu(\psi(x, \sigma(y))) = \psi^*(\sigma(x), y) = -\psi(y, \sigma(x))$. If we let $\phi(x, y) = \psi(x, \sigma(y))$ for all $x, y \in H$, then $\mu \circ \phi = \phi^*$. The converse is obvious. □

Corollary 7.2. *Let $\psi : H \times H \to N$ be an additive Hadamard cocycle and $|N|$ be odd. The design $\mathfrak{D}_\psi$ has a polarity if and only if ψ is isotopic to an additive Hadamard cocycle $\phi : H \times H \to N$ such that there are two subgroups N_1 and N_2 of N with $N = N_1 \oplus N_2$, i.e. $N_1 \cap N_2 = 0$ and $N = N_1 + N_2$, two additive Hadamard cocycles $\phi_1 : H \times H \to N_1$ with $\phi_1 = -\phi_1^*$ and $\phi_2 : H \times H \to N_2$ with $\phi_2 = \phi_2^*$ and $\phi = \phi_1 \oplus \phi_2$.*

Proof. By Theorem 7.1, ψ is isotopic to an additive Hadamard cocycle ϕ with $\mu(\phi) = \phi^*$ for some $\mu \in \mathrm{Aut}(N)$ satisfying $\mu^2 = 1$. Since $|N|$ is odd, we can define $N_1 = \mathrm{Im}[(1-\mu)/2]$ and $N_2 = \mathrm{Im}[(1+\mu)/2]$, $\phi_1 = \frac{1-\mu}{2} \circ \phi$ and $\phi_2 = \frac{1+\mu}{2} \circ \phi$. One can easily check that N_1, N_2, ϕ_1 and ϕ_2 satisfy all conditions in the corollary and by Proposition 3.4, the cocycles ϕ_1 and ϕ_2 are Hadamard cocycles. Obviously $\phi = \phi_1 \oplus \phi_2$. The converse is also clear. □

Corollary 7.3. *Let $\psi : H \times H \to N$ be an additive Hadamard cocycle. The design $\mathfrak{D}_\psi$ has an absolute polarity if and only if ψ is isotopic to an additive Hadamard cocycle $\phi : H \times H \to N$ such that $\phi = \phi^*$ and $\phi(x, x) = 0$ for all $x \in H$.*

Proof. If $\iota : \mathfrak{D}_\psi \to \mathfrak{D}_\psi^*$ is a polarity given by $a, a^* \in H$, $b \in N$, $\sigma, \sigma^* \in \mathrm{Aut}(H)$, $\mu \in \mathrm{Aut}(N)$ such that $\mu(\psi(x, y)) = \psi^*(\sigma(x), \sigma^*(y))$, by the proof of Theorem 7.1 we have $\sigma^* = \sigma^{-1}$, $a^* = -\sigma^{-1}(a)$, $\mu^2 = 1$, $\mu(b) = -b$. By (24), we get a permutation ι_f of $F(\mathfrak{D}_\psi)$ given by

$$\begin{aligned}\iota_f(m, x, y) = \big(&\sigma(x) + a, \sigma^{-1}(m - a), \mu(y) + b + \psi\big(\sigma^{-1}(a), \sigma(x)\big) \\ &+ \psi\big(\sigma^{-1}(m - a), \sigma(x) + a\big)\big)\end{aligned}$$

for all $(m, x, y) \in F(\mathfrak{D}_\psi)$. The polarity ι is an absolute polarity if and only if for each $x \in H$ and $y \in N$, there is a unique $m \in H$ such that $\iota_f(m, x, y) = (m, x, y)$, that is $m = \sigma(x) + a$ and

$$\begin{aligned}y &= \mu(y) + b + \psi\big(\sigma^{-1}(a), \sigma(x)\big) + \psi\big(\sigma^{-1}(m - a), \sigma(x) + a\big) \\ &= \mu(y) + b + \psi\big(\sigma^{-1}(a), \sigma(x)\big) + \psi\big(x, \sigma(x) + a\big) \\ &= \mu(y) + b + \psi\big(\sigma^{-1}(a), \sigma(x)\big) + \psi(x, a) + \psi\big(x, \sigma(x)\big)\end{aligned}$$

for all $x \in H$ and $y \in N$. Let $y = 0$, we get $b + \psi(\sigma^{-1}(a), \sigma(x)) + \psi(x, a) + \psi(x, \sigma(x)) = 0$ for all $x \in H$. Therefore $b = 0$, $\psi(\sigma^{-1}(a), \sigma(x)) + \psi(x, a) + \psi(x, \sigma(x)) = 0$ for all $x \in H$, $\mu(y) = y$ for all $y \in N$. This implies that $\mu = 1$, and

$$\psi\big(\sigma^{-1}(a), \sigma(x)\big) + \psi(x, a) = \mu\big(\psi\big(\sigma^{-1}(a), \sigma(x)\big)\big) + \psi(x, a) = \psi^*(a, x) + \psi(x, a) = 0,$$

and therefore $\psi(x, \sigma(x)) = 0$ for all $x \in H$. Hence the additive Hadamard cocycle $\phi : H \times H \to N$ given by $\phi(x, y) = \psi(x, \sigma(y))$ satisfies $\phi = \phi^*$ and $\phi(x, x) = 0$ for all $x \in H$. □

Remark 7.4. Corollary 7.3 shows that the additive Hadamard cocycles studied in [7] are the prototypical additive Hadamard cocycles whose divisible designs admit absolute polarities.

8. Relative difference sets in flag groups of odd orders and elementary abelian groups

In this section we show that flag groups of odd orders can be obtained from intertwining products of additive Hadamard cocycles and their dual cocycles, and hence there are semi-regular relative difference sets in these groups. We also demonstrate that if we apply the same twisted intertwining product construction to additive Hadamard cocycles of elementary abelian 2-groups, we obtain bent functions. We then finish this paper with two questions concerning $\mathbb{F}_2$ valued bent functions.

If we take a closer look at the multiplication (11) of the flag group $\mathrm{Flag}(\psi)$ of the additive Hadamard cocycle $\psi : H \times H \to N$, it is easy to see that $\mathrm{Flag}(\psi) = E(H \times H, N, 0 \boxtimes \psi)$, where 0 is the trivial cocycle. In order to have a better understanding of the structure of the flag groups, we need the following two simple lemmas.

Lemma 8.1. *If $\psi : H \times H \to N$ is a cocycle and $\mu \in \mathrm{Aut}(N)$, then $\mu \circ \psi : H \times H \to N$ is also a cocycle and $E(H, N, \psi) \cong E(H, N, \mu \circ \psi)$.*

Lemma 8.2. *If $\psi : H \times H \to N$ is a multiplicative cocycle, then $(-\psi) \boxtimes \psi^* = \partial\psi$ is a coboundary.*

By Theorem 4.9 and covering subgroups of Davis and Jedwab [10], we get an interesting consequence of Lemma 8.2.

Theorem 8.3. *Let H and N be two additive elementary abelian p-groups, and $\psi : H \times H \to N$ be an additive cocycle. Then the following statements are equivalent.*

(i) *The cocycle ψ is a Hadamard cocycle.*
(ii) *The cocycle ψ as a function from $H \times H$ to N is a bent function, i.e. $\partial\psi$ is a Hadamard cocycle.*
(iii) *For each function $g : H \to N$, the function $\psi(x, y) + g(y)$ from $H \times H$ to N is a bent function.*
(iv) *For each function $g : H \to N$ and each permutation γ of H, the function $\psi(x, \gamma(y)) + g(y)$ from $H \times H$ to N is a bent function.*

Proof. The equivalence of (i) and (ii) is a direct consequence of Theorem 4.9 and Lemma 8.2. The equivalence of (i) and (iii) is from Theorem 4.9, Lemma 8.2, and the fact that if $f(x, y) = \psi(x, y) + g(y)$, then $\partial f = \partial\psi + \partial g = (-\psi) \boxtimes_{\partial g} \psi^*$. In order to see that (i) implies (iv), we need to look at the character sum of the graph G_f of the function $f(x, y) = \psi(x, \gamma(y)) + g(y)$.

The graph

$$G_f = \big\{\big(x, y, \psi\big(x, \gamma(y)\big) + g(y)\big) \bigm| x, y \in H\big\} = \bigcup_{y \in H} \big(L_y + \big(0, y, g(y)\big)\big),$$

where $L_y = \{(x, 0, \psi(x, \gamma(y))) \mid x \in H\}$ is a subgroup of order $|H|$ in $H \times H \times N$ as ψ is an additive cocycle, and $L_y + (0, y, g(y))$ is a coset of L_y obtained from a translation of L_y in $H \times H \times N$ by the element $(0, y, g(y)) \in H \times H \times N$. If we let $L_\infty = \{(0, 0, z) \mid z \in N\}$, then the subgroups in $\{L_y \mid y \in H \cup \{\infty\}\}$ form covering subgroups of $H \times \{0\} \times N$, that is for each non-principal character χ of $H \times \{0\} \times N$, it is trivial on exactly one subgroup in $\{L_y \mid y \in H \cup \{\infty\}\}$. This can be checked by verifying that every pair of two distinct subgroups L_{y_1} and L_{y_2} generates $H \times \{0\} \times N$ as ψ is a Hadamard cocycle, and that the summation of numbers of prime index subgroups in $H \times \{0\} \times N$ containing L_y over all $y \in H \cup \{\infty\}$ is precisely the total number of prime index subgroups in $H \times \{0\} \times N$. This implies that G_f is a semi-regular relative difference set in $H \times H \times N$ relative to L_∞ and $f(x, y) = \psi(x, \gamma(y)) + g(y)$ is a bent function. □

We call functions in (iv) of Theorem 8.3 the *Maiorana–McFarland functions of the additive cocycle ψ*. When ψ is the standard inner product with respect to a basis of H and $N = \mathbb{Z}/p\mathbb{Z}$, these functions are the classic Maiorana–McFarland functions.

Now if $|N|$ is odd and $\psi : H \times H \to N$ is a multiplicative cocycle, then by Lemmas 8.1 and 8.2 and isomorphism in (4), one has

$$\begin{aligned} E(H \times H, N, 0 \boxtimes \psi) &\cong E\big(H \times H, N, 2(0 \boxtimes \psi)\big) \\ &\cong E\big(H \times H, N, 0 \boxtimes (2\psi)\big) \\ &\cong E\big(H \times H, N, 0 \boxtimes (2\psi) + \partial\big(-\psi^*\big)\big) \\ &\cong E\big(H \times H, N, 0 \boxtimes (2\psi) + \psi^* \boxtimes (-\psi)\big) \\ &\cong E\big(H \times H, N, \psi^* \boxtimes \psi\big). \end{aligned}$$

Therefore when $\psi : H \times H \to N$ is an additive Hadamard cocycle and $|N|$ is odd, the flag group $\mathrm{Flag}(\psi) \cong E(H \times H, N, \psi^* \boxtimes \psi)$. By Corollary 3.2 and Theorem 4.9, the cocycle $\psi^* \boxtimes \psi$ is also an additive Hadamard cocycle and satisfies $(\psi^* \boxtimes \psi)^* = \psi^* \boxtimes \psi$. This type of Hadamard cocycle was studied in detail in [7] and results of [7] implies that

Theorem 8.4. *If $\psi : H \times H \to N$ is an additive Hadamard cocycle and $|N|$ is odd, then the flag group $\mathrm{Flag}(\psi)$ is a special p-group of exponent p with $|Z(\mathrm{Flag}(\psi))| + |\mathrm{Flag}(\psi)/Z(\mathrm{Flag}(\psi))| - 1$ conjugacy classes, where $Z(\mathrm{Flag}(\psi))$ is the center of $\mathrm{Flag}(\psi)$, and up to equivalence $\mathrm{Flag}(\psi)$ contains a unique semi-regular relative difference set R relative to $Z(\mathrm{Flag}(\psi))$ such that $1 \in R$ and $rRr = R$ for all $r \in R$ and the design $\mathfrak{D}_R$ admits an absolute polarity.*

If $|N|$ is even, i.e. H and N are elementary abelian 2-groups, the cocycle

$$\psi^* \boxtimes \psi = \psi^* \boxtimes (-\psi) = \partial\big(-\psi^*\big) = \partial\big(\psi^*\big),$$

and therefore $E(H \times H, N, \psi^* \boxtimes \psi) \cong H \times H \times N$ is an elementary abelian group, which is no longer isomorphic to the flag group $\mathrm{Flag}(\psi)$. However the group $E(H \times H, N, \psi^* \boxtimes \psi)$ contains a semi-regular relative difference set because $\psi^* \boxtimes \psi$ is a Hadamard cocycle. Since $\psi^* \boxtimes \psi = \partial(\psi^*)$, the function $\psi^* : H \times H \to N$ is a bent function. Unlike the $|N|$ odd case, relative difference sets in an elementary abelian 2-group are not unique up to equivalence. We now describe some examples of (q^2, q, q^2, q)-relative difference sets in elementary abelian groups constructed by Nyberg [26] generalizing the methods of Dillon [11,12] and McFarland [24].

Let $\mathbb{F} = \{x_1, x_2, \ldots, x_q\}$ be a finite field with q elements and $\{L_0, L_1, \ldots, L_q\}$ be a spread of $\mathbb{F} \times \mathbb{F}$, i.e. each L_i is a subgroup of order q in $\mathbb{F} \times \mathbb{F}$, and for each $i \neq j$, $\langle L_i, L_j\rangle = \mathbb{F} \times \mathbb{F}$, or equivalently $L_i \cap L_j = \{(0,0)\}$. Using character sum, one can easily check that the following subsets R_1 and R_2 are (q^2, q, q^2, q)-relative difference set in $\mathbb{F}^3$. They are generally inequivalent since the construction of R_1 is analogous to McFarland's construction [24] while the construction of R_2 is in the spirit of Dillon's construction [11,12].

Example 8.5. The set

$$R_1 = \bigcup_{i=1}^{q} (x_i, L_i)$$

is a (q^2, q, q^2, q)-relative difference set in $\mathbb{F}^3$ relative to the subgroup $\{(0, y, z) \mid (y, z) \in L_0\}$.

Example 8.6. The set

$$R_2 = (x_1, L_0) \cup \bigcup_{i=1}^{q} \big(x_i, L_i \setminus \big\{(0,0)\big\}\big)$$

is a (q^2, q, q^2, q)-relative difference set in $\mathbb{F}^3$ relative to the subgroup $\{(x, 0, 0) \mid x \in \mathbb{F}\}$.

A semi-regular relative difference set in an elementary abelian group $H \times N = \mathbb{Z}_p^l$ relative to N is simply a bent function from H to N, and Corollary 4.2 shows that this one single function is equivalent to an elementary abelian group of bent functions from H to $\mathbb{Z}_p$ which is isomorphic to N.

Since each spread in $\mathbb{F} \times \mathbb{F}$ corresponds to a quasifield, the bent function in Example 8.5 is obtained from the multiplication of the quasifield while the bent function in Example 8.6 is obtained from the one sided division of the quasifield. For instance if the quasifield multiplication is given by $x * y = x\gamma(y)$ for some permutation γ of $\mathbb{F}$ that fixes 0 and 1, then the function $f_1(x, y) = x\gamma(y)$ can be a bent function of Example 8.5 and $f_2(x, y) = \gamma^{-1}(xy^{q-2})$ can be a bent function of Example 8.6. It is well known that the order of any group of bent functions from H to $\mathbb{Z}_p$ is no larger than the order of H, and when it is equal to the order of H, we obtain a planar function. When H is an elementary abelian 2-group, it is shown by Nyberg [26], and later by Ma [23] in a more general setting, that the order of any group of bent functions from H to $\mathbb{Z}_2$ is no larger than $\sqrt{H}$. We conclude this paper with the following questions:

Question 8.7. Does every bent function from H to $\mathbb{Z}_2$ belong to a group of bent functions of order greater 2? For example, does the bent functions obtained from Kasami functions in [13] belong to a larger group of bent functions?

Question 8.8. Does every bent function from H to $\mathbb{Z}_2$ belong to a group of bent functions of order $\sqrt{H}$?

Acknowledgments

The author thanks J.F. Dillon for pointing out to him Ref. [26]. The author also thanks referees for their careful reading of the manuscript and their comments and suggestions. This research is partially supported by a Wright State University Research Initiation Grant.

References

[1] A.A. Albert, Non-associative algebras I. Fundamental concepts and isotopy, Ann. of Math. 43 (1942) 685–707.
[2] A.A. Albert, Finite division algebras and finite planes, in: Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., 1960, pp. 53–70.
[3] K.T. Arasu, D. Jungnickel, A. Pott, Divisible difference sets with multiplier −1, J. Algebra 133 (1990) 35–62.
[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. 1, 2nd ed., Cambridge University Press, Cambridge, 1999.
[5] K.S. Brown, Cohomology of Groups, Springer, New York, Heidelberg, Berlin, 1982.
[6] Y.Q. Chen, Twisted product of cocycles and factorization of semi-regular relative difference sets, J. Combin. Des. 16 (2008) 431–441.
[7] Y.Q. Chen, K.J. Horadam, W.-H. Liu, Relative difference sets fixed by inversion III—cocycle theoretical approach, Discrete Math. 308 (2008) 2764–2775.
[8] Y.Q. Chen, C.H. Li, Relative difference sets fixed by inversion and Cayley graphs, J. Combin. Theory Ser. A 111 (2005) 165–173.
[9] Y.Q. Chen, D.K. Ray-Chaudhuri, Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings II, J. Combin. Theory Ser. A 76 (1996) 179–196.
[10] J.A. Davis, J. Jedwab, A unifying construction for difference sets, J. Combin. Theory Ser. A 80 (1997) 13–78.
[11] J.F. Dillon, Elementary Hadamard difference sets, PhD thesis, University of Maryland, 1974.
[12] J.F. Dillon, Elementary Hadamard difference sets, in: Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Florida Atlantic Univ., Boca Raton, FL, 1975, in: Congressus Numerantium, vol. XIV, Utilitas Math., Winnipeg, MB, 1975, pp. 237–249.
[13] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342–389.
[14] J.C. Galati, A group extensions approach to relative difference sets, J. Combin. Des. 12 (2004) 279–298.
[15] Y. Hiramine, Planar functions and related group algebras, J. Algebra 152 (1992) 135–145.
[16] Y. Hiramine, On planar functions, J. Algebra 133 (1990) 103–110.
[17] Y. Hiramine, Automorphisms of p-groups of semifield type, Osaka J. Math. 20 (1983) 735–746.
[18] K.J. Horadam, W. de Launey, Cocyclic development of designs, J. Algebraic Combin. 2 (1993) 267–290.
[19] D. Jungnickel, On automorphism groups of divisible designs, Canad. J. Math. 34 (1982) 257–297.
[20] W.-H. Liu, Y.Q. Chen, K.J. Horadam, Relative difference sets fixed by inversion II—character theoretical approach, J. Combin. Theory Ser. A 111 (2005) 175–189.
[21] K.H. Leung, S.L. Ma, V. Tan, Planar functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$, J. Algebra 224 (2000) 427–436.
[22] S.L. Ma, Planar functions, relative difference sets, and character theory, J. Algebra 185 (1996) 342–356.
[23] S.L. Ma, Reversible relative difference sets, Combinatorica 12 (1992) 425–432.
[24] R.L. McFarland, A family of difference sets in non-cyclic abelian groups, J. Combin. Theory Ser. A 15 (1973) 1–10.
[25] S.L. Ma, A. Pott, Relative difference sets, planar functions, and generalized Hadamard matrices, J. Algebra 175 (1995) 505–525.

[26] K. Nyberg, Perfect nonlinear S-boxes, in: Advances in Cryptology—EUROCRYPT' 91, Brighton, 1991, in: Lecture Notes in Comput. Sci., vol. 547, Springer, Berlin, 1991, pp. 378–386.
[27] A.A.I. Perera, K.J. Horadam, Cocyclic generalised Hadamard matrices and central relative difference sets, Des. Codes Cryptogr. 15 (1998) 187–200.
[28] A. Pott, Finite Geometry and Character Theory, Lecture Notes in Math., vol. 1601, Springer, Berlin, Heidelberg, 1995.
[29] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 2 (1976) 300–305.